BLACK BOX GROUPS AND RELATED GROUP THEORETIC CONSTRUCTIONS

ŞÜKRÜ YALÇINKAYA

JUNE 2007

BLACK BOX GROUPS AND RELATED GROUP THEORETIC CONSTRUCTIONS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

ŞÜKRÜ YALÇINKAYA

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
MATHEMATICS

JUNE 2007

Approval of the Graduate School of Natural and Applied Sciences

Prof. Dr. Canan ÖZGEN
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Doctor of Philosophy.

Prof. Dr. Zafer NURLU
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Doctor of Philosophy.

Prof. Dr. Alexandre BOROVIK	Assoc. Prof. Dr. Ayşe BERKMAN
Co-Supervisor	Supervisor

Examining Committee Members

Prof. Dr. Mahmut KUZUCUOĞLU	(METU)	_____
Assoc. Prof. Dr. Ayşe BERKMAN	(METU)	_____
Prof. Dr. Alexandre BOROVIK	(Manchester Univ.)	_____
Prof. Dr. Mehpare BİLHAN	(METU)	_____
Assoc. Prof. Dr. Feride KUZUCUOĞLU	(Hacettepe Univ.)	_____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name : Şükrü Yalçınkaya
Signature :

Abstract

BLACK BOX GROUPS AND RELATED GROUP THEORETIC CONSTRUCTIONS

YALÇINKAYA, Şükrü
Ph.D., Department of Mathematics
Supervisor: Assoc. Prof. Dr. Ayşe BERKMAN
Co-Supervisor: Prof. Dr. Alexandre BOROVIK

JUNE 2007, 86 pages

The present thesis aims to develop an analogy between the methods for recognizing a black box group and the classification of the finite simple groups. We propose a uniform approach for recognizing simple groups of Lie type which can be viewed as the computational version of the classification of the finite simple groups. Similar to the inductive argument on centralizers of involutions which plays a crucial role in the classification project, our approach is based on a recursive construction of the centralizers of involutions in black box groups. We present an algorithm which constructs a long root $\mathrm{SL}_2(q)$-subgroup in a finite simple group of Lie type of odd characteristic p extended possibly by a p-group. Following this construction, we take the Aschbacher's "Classical Involution Theorem" as a model in the final recognition algorithm and we propose an algorithm which constructs all root $\mathrm{SL}_2(q)$-subgroups corresponding to the nodes in the extended Dynkin diagram, that is, our approach is the construction of the the extended Curtis - Phan - Tits presentation of the finite simple groups of Lie type of odd characteristic which further yields the construction of all subsystem subgroups which can be read from the extended Dynkin diagram. In this thesis, we present this algorithm for the groups $\mathrm{PSL}_n(q)$ and $\mathrm{PSU}_n(q)$. We also present an algorithm which determines whether the p-core (or "unipotent radical") $O_p(G)$ of a black box group G is trivial or not where $G/O_p(G)$ is a finite sim-

ple classical group of Lie type of odd characteristic p answering a well-known question of Babai and Shalev.

The algorithms presented in this thesis have been implemented extensively in the computer algebra system GAP.

Keywords: Black Box Groups, Groups Of Lie Type.

Öz

KARA KUTU GRUPLARI VE İLGİLİ GRUP KURAMSAL İNŞAALARI

YALÇINKAYA, Şükrü
Doktora, Matematik Bölümü
Tez Yöneticisi: Doç. Dr. Ayşe BERKMAN
Ortak Tez Yöneticisi: Prof. Dr. Alexandre BOROVIK

Haziran 2007, 86 sayfa

Bu tez bir kara kutu grubunun tanınması ile sonlu basit grupların sınıflandırılmasında kullanılan metodlar arasındaki analojiyi kurmayı amaçlamaktadır. Sonlu basit kara kutu Lie tipi gruplarının tanınması için sonlu basit grupların sınıflandırılmasının berimsel versiyonu olarak görülebilen bir yaklaşım öneriyoruz. Sınıflandırma projesinde çok önemli bir rol oynayan özters elemanların değişim grupları üzerinde tümevarımsal argümanlara benzer şekilde, yaklaşımımız özters elemanların değişim gruplarının tekrarlamalı inşaalarına dayanmaktadır. Karakteristiği tek sayı p olan p-group ile genişletilmiş sonlu basit Lie tipi gruplarında uzun kök $\mathrm{SL}_2(q)$-gruplarının inşaası için bir algoritma sunuyoruz. Bu inşaayı takiben, son tanınma algoritması için Aschbacher'in "Klasik Özters Teorem"ini model alıp genişletilmiş Dynkin diyagramındaki noktalara karşılık gelen bütün kök $\mathrm{SL}_2(q)$-altgruplarını inşaa eden bir algoritma geliştiriyoruz, bir başka deyişle yaklaşımımız ileride genişletilmiş Dynkin diyagramından okunabilen bütün altsistem altgruplarının inşaası olacak olan genişletilmiş Curtis - Phan - Tits sisteminin inşaasıdır. Bu tezde, bu algoritmayı $\mathrm{PSL}_n(q)$ ve $\mathrm{PSU}_n(q)$ grupları için sunacağız. Ayrıca Babai ve Shalev'in ünlü problemini yanıtlayan p-özüne bölündüğünde sonlu basit klasik kara kutu Lie tipi gruplarının p-özünün birim grup olup olmadığına karar veren bir algoritma sunuyoruz.

Bu tezde sunulan algoritmalar cebir bilgisayar sistemi olan GAP'ta prog-

ramlanarak kapsamlı bir şekilde test edilmiştir.

Anahtar Kelimeler: Kara Kutu Grupları, Lie Tipi Grupları.

To my family

ACKNOWLEDGEMENTS

I am deeply indebted to my supervisors Ayşe Berkman and Alexandre Borovik for their guidance and constant encouragement. I would like to express my deepest gratitude to Ayşe Berkman for her continuous motivation and support starting from my undergraduate years. I can not overstate how Alexandre Borovik's inspiring ideas and invaluable suggestions improved my visions in all aspects, and I am extremely grateful to him for sharing his knowledge and experiences generously.

I would like to thank to Tuna Altınel and Frank Wagner for their very kind invitation to visit Université Claude Bernard Lyon 1 where I made great progress. I am grateful to Tuna Altınel for taking care of my numerous problems and letting me concentrate on my work only.

My special thanks are due to Emrah Çakçak who made very positive contribution both morally and mathematically at every stages. I would like to thank to Erol Serbest for his invaluable advice on many issues. I would also like to thank to Murat Vatansever, İnanç Kanık, Ali Fıkırkoca and Mahruf Chowdhury for their great help during difficult times. I wish to thank all my friends in Ankara, Manchester and Lyon who took part in one way or another in the preparation of this thesis.

I would like to acknowledge University of Manchester and Université Claude Bernard Lyon 1 for providing me excellent studying environment during my stays, and also I gratefully acknowledge the financial support from TÜBİTAK and MATHLOGAPS.

I would like to thank to the members of the examining committee.

I am extremely grateful to my family for their continuous support and encouragement during this long period of study.

Table of Contents

Chapter 1

Introduction

The present thesis aims to develop an analogy between the methods for recognizing a black box group and the classification of the finite simple groups. The centralizers of involutions, which played a prominent role in the classification of the finite simple groups, are the main focus of our methods presented in this work.

The problems in computational group theory are centered around to develop efficient algorithms for understanding structural properties of finite groups. One of the major goals is to develop an algorithm which constructs the composition series of a given group. When the group representation is known, for example, generators of a group may be given as permutations on some set or matrices over finite fields, the algorithms, in many cases, depend on the representation of the given group. If the group is known to be a permutation group, there is a huge library of algorithms running in nearly linear-time in the input length (for example, constructing centralizers of elements, center of the group etc., see [46] for an exposition). The composition series of a given permutation group $G = \langle S \rangle \leqslant \mathrm{Sym}(n)$ can be constructed in time $O(n|S| \log^c |G|)$ where c is a universal constant [46, Section 6.2]. In principle, the methods for the matrix group algorithms are different from those of the permutation group algorithms. Babai and Szemerédi generalized the group algorithms by introducing *black box group* theory and they applied it to the matrix groups over finite fields [11].

A *black box group* G is a group equipped with a black box ('oracle') where the group operations are performed by the oracle. The elements of the black box groups are encoded as $0-1$ strings of uniform length, say N. Given strings representing $g, h \in G$, the oracle can compute the strings representing $g \cdot h$, g^{-1} and decide whether $g = h$. Thus we have an upper bound for the order of the group $|G| \leqslant 2^N$. The central examples for black box groups are permutation groups and matrix groups over finite fields where the input sizes are $N = |S|n$ (n is the size of the permutation domain) and $N = |S|n^2 \log q$ (n is the size of the square matrices and q is the size of the underlying field)

respectively, here $G = \langle S \rangle$. The black box group algorithms do not depend on the specific features of the group representation or how the group operations are performed [46]. In this setting, as the black box group operations allow only to work with the multiplication table of the input group, it is almost impossible, for example, in big matrix groups, to get information about the group without an additional information or oracle. One can overcome this difficulty, for example, by assuming an *order oracle* with which we can find the orders of elements, or in the case of finite classical groups the dimension of the underlying vector space and the size of the field can be taken as an input.

A black box group algorithm for the construction of composition series is proposed in [7]. Every finite group G has a series of characteristic subgroups

$$1 \leqslant \mathrm{Sol}(G) \leqslant \mathrm{Soc}^*(G) \leqslant \mathrm{Pker}(G) \leqslant G, \tag{1.1}$$

where $\mathrm{Sol}(G)$ is the largest soluble normal subgroup of G, $\mathrm{Soc}^*(G)$ is defined by

$$\mathrm{Soc}^*(G)/\mathrm{Sol}(G) = \mathrm{Soc}(G/\mathrm{Sol}(G)),$$

where $\mathrm{Soc}(G)$, the product of the minimal normal subgroups of G, is semisimple. Let $\mathrm{Soc}^*(G)/\mathrm{Sol}(G) = T_1 \times \ldots \times T_k$ where the T_i are nonabelian simple groups, then G acts on $\{T_1, \ldots, T_k\}$ by conjugation and $\mathrm{Pker}(G)$ is defined to be the kernel of this action. Now

1. $\mathrm{Sol}(G)$ is soluble,
2. $\mathrm{Soc}^*(G)/\mathrm{Sol}(G)$ is semisimple,
3. $\mathrm{Pker}(G)/\mathrm{Soc}^*(G) \leqslant \mathrm{Out}(T_1) \times \ldots \times \mathrm{Out}(T_k)$ is soluble by Schreier conjecture,
4. $G/\mathrm{Pker}(G) \leqslant \mathrm{Sym}(k)$, symmetric group on k-letters.

Now the composition series of G can be obtained from the refinement of the chain (1.1). Babai and Beals [7] presented an algorithm which constructs for a black box group G, the $\mathrm{Pker}(G)$, the factors of $\mathrm{Soc}^*/\mathrm{Sol}(G)$, in particular, they constructed the non-abelian composition factors of $G/\mathrm{Sol}(G)$ in polynomial time in the input length. The group $G/\mathrm{Pker}(G)$ is a permutation group and the composition factors can be constructed by an algorithm in [46, Section 6.2]. The subgroups $\mathrm{Pker}(G)/\mathrm{Soc}^*(G)$ and $\mathrm{Sol}(G)$ are soluble,

therefore they contribute only abelian composition factors. The missing part in this algorithm is the construction of $\mathrm{Sol}(G)$, even the decision problem whether $\mathrm{Sol}(G) = 1$ is not answered.

The project on the construction of composition factors of a given matrix group over finite fields is known as the "computational matrix group project" [36], and Leedham–Green outlined in [36] how a composition series for a matrix group $G \leqslant \mathrm{GL}_n(q)$ can be computed by using Aschbacher's classification theorem on the subgroup structure of $\mathrm{GL}_n(q)$ [4]. The algorithm is recursive, and if G is not simple, it first decides the families of Aschbacher's classification where G belongs to, and then constructs a proper normal subgroup $N \trianglelefteq G$ and a presentation for the quotient group G/N. In order that the recursive argument works, it is essential to have a *constructive recognition algorithm* for each finite simple group $G = \langle S \rangle$. The constructive recognition algorithm for a simple group $G = \langle S \rangle$ is an algorithm which solves the following

1. Determine the isomorphism type of G.
2. Construct an explicit isomorphism between G and its standard copy.
3. Express any element $g \in G$ as a word in S.

The first of the recognition algorithms for finite groups is presented in [42] which decides whether a given matrix group $G \leqslant \mathrm{GL}_n(q)$ for known n and q contains $\mathrm{SL}_n(q)$. An example of a constructive recognition first appeared in [21] for the group $G = \mathrm{SL}_n(q)$ in its natural representation, that is, G is given as $n \times n$ invertible matrices over a field of order q. A breakthrough result, which does not use any specific properties of the given group representation, that is, black box group algorithm, is the algorithm for $\mathrm{PSL}_n(2)$ [24]. Following this algorithm Kantor and Seress developed constructive black box group algorithms to all classical groups [34], however these algorithms are not polynomial time algorithms in the input length, they are polynomial time algorithms in q but the input size involves only $\log q$. These algorithms depend on the construction of p-elements (or "unipotent elements"). However the share of p'-elements (or "semisimple elements") in a simple group of Lie type defined over a field $\mathbb{F}_q$ is $1 - O(1/q)$ [28]. Therefore the probability of a random element to be semisimple is close to 1 when the order of the field is *large*, in other words, it is unrealistic to expect producing unipotent elements over large fields by random search. Later the algorithms

in [34] were upgraded to polynomial time constructive recognition algorithms [15, 16, 17] by assuming additional oracles: discrete logarithm oracle in $\mathbb{F}_q^*$ and $\mathrm{SL}_2(q)$-oracle, that is, constructive recognition of $\mathrm{SL}_2(q)$ is assumed. Therefore these papers reduce the constructive recognition problem for black box classical groups to the constructive recognition of $\mathrm{SL}_2(q)$. Recently, in the case of a matrix group, a constructive recognition algorithm for $\mathrm{SL}_2(q)$ has been developed [23] by assuming a discrete logarithm problem on $\mathbb{F}_q^*$.

The algorithms for determining the isomorphism type of G are called *probabilistic recognition algorithms* and constitute an important part of the constructive recognition algorithm. That is, the first step in the constructive recognition algorithms for the finite simple groups is to determine the isomorphism type of the group and once the standard name of the group is known then construct an isomorphism between the input group and its standard copy. A probabilistic recognition algorithm for finite simple groups of Lie type, namely, the computation of their standard names, is presented in [9] by using the order oracle. The idea is based on the analysis of the statistics of element orders, which are distinct for each Lie type group except for the groups $\mathrm{PSp}_{2n}(q)$ and $\Omega_{2n+1}(q)$, q odd. This approach fails for the groups $\mathrm{PSp}_{2n}(q)$ and $\Omega_{2n+1}(q)$, q odd, because when the size of the field is large, a random element is regular semisimple with probability close to 1 and the statistics of orders of regular semisimple elements are virtually the same for these groups, see [1] for a thorough discussion. To complete the recognition problem for all finite simple groups of Lie type Altseimer and Borovik presented an algorithm distinguishing $\mathrm{PSp}_{2n}(q)$ from $\Omega_{2n+1}(q)$, q odd, which is based on the structure of the centralizers of involutions and the conjugacy classes in these groups [1].

An algorithm for finding the characteristic of the underlying field for the groups of Lie type is proposed in [35] by assuming an order oracle. Therefore combining the algorithms in [1, 9, 35] with the algorithm in [7], the standard names of the non-abelian composition factors of the black box groups can be determined in polynomial time. Moreover, every simple group can be recognized among all simple groups. The question of recognizing simplicity of a given black box group is studied in [10], and determining whether a black box group X is simple or not is reduced in polynomial time to determining whether $O_p(X) \neq 1$ [10] which is a part of this thesis.

The algorithms so-called *verification algorithms* are also useful in many cases. For example, if an element in a black box group G is found whose order is not present in a known finite group X, then clearly $G \ncong X$. In this

thesis, we frequently use these types of algorithms.

1.1 Algorithmic preliminaries

An algorithm is called a *randomized algorithm* if it makes random choices during its execution. A randomized algorithm has the worst-case success probability ε, for $0 < \varepsilon < 1$, if, for every problem instance, the algorithm returns a correct answer with probability at least ε.

A *Monte–Carlo algorithm* is a randomized algorithm which gives a correct output to a decision problem with probability strictly bigger than $1/2$. The probability of having incorrect output can be made arbitrarily small by running the algorithm sufficiently many times. A Monte–Carlo algorithm with outputs "yes" and "no" is called *one-sided* if the output "yes" is always correct. A *polynomial time* algorithm is an algorithm whose running time is polynomial in the input length. A Monte–Carlo algorithm which runs in polynomial time in the input length is called a *Monte–Carlo polynomial time algorithm*.

Let f and g be two functions on $\mathbb{N}$. Then we write

1. $f(n) = O(g(n))$ if there exists a positive constant c and a natural number n_0 such that $0 \leqslant f(n) \leqslant cg(n)$ for all $n \geqslant n_0$

2. $f(n) = \Theta(g(n))$ if there exist positive constants c_1 and c_2, and a natural number n_0 such that $c_1 g(n) \leqslant f(n) \leqslant c_2 g(n)$ for all $n \geqslant n_0$

1.2 Random elements

The crucial part in a black box group algorithm is the construction of uniformly distributed random elements in the group. Babai proposed an algorithm which, although not practical, supplies a theoretical justification that *nearly* uniformly distributed elements can be constructed [6]. This algorithm first constructs a new generating set of $O(\log |G|)$ elements in $O(\log^5 |G|)$ multiplications and then uses this set to produce sequence of nearly uniformly distributed elements in $O(\log |G|)$ multiplications for each element. Here, an algorithm outputs a nearly uniformly distributed element x in a group G if $(1-\varepsilon)/|G| \leqslant \mathrm{Prob}(x = g) \leqslant (1+\varepsilon)/|G|$ for all $g \in G$ and $\varepsilon \leqslant 1/2$.

On the practical side, there is "the product replacement algorithm" [22]. Let $\Gamma_k(G)$ be the graph whose vertices are generating k-tuples of elements in G and edges are given by the following transformations:

$$\begin{aligned}(g_1,\ldots,g_i,\ldots,g_k) &\to (g_1,\ldots,g_i\cdot g_j^{\pm 1},\ldots,g_k)\\ (g_1,\ldots,g_i,\ldots,g_k) &\to (g_1,\ldots,g_j^{\pm 1}\cdot g_i,\ldots,g_k)\end{aligned}$$

Note that $i\neq j$ above, and therefore these transformations map a generating k-tuple to generating k-tuple. A 'random' element in G can be produced in the following way. Apply these transformations randomly and return a random component of the resulting generating k-tuple. The connectivity of $\Gamma_k(G)$ and the mixing time of this algorithm are the main obstacles to construct random elements in this way.

The mixing time for a random walk on a graph Γ is the minimal number of steps such that after these steps

$$\frac{1}{2}\sum_{v\in\Gamma}\left|\text{Prob}(\text{ending at } v)-\frac{1}{\#\Gamma}\right|<\frac{1}{e}$$

which means that the distribution of the end points of the random walk on this graph is close to the uniform distribution. It is proved in [43] that the mixing time for a random walk on $\Gamma_k(G)$ is polynomial in k and $\log|G|$ when k is sufficiently large. Indeed, when $k=\Theta(\log|G|\log\log|G|)$ the mixing time of the walk is $O(\log^9|G|(\log\log|G|)^5)$.

Note that it is essential that the graph $\Gamma_k(G)$ is connected to produce random elements by this procedure. Although $\Gamma_k(G)$ is not always connected, which can be observed from elementary abelian p-groups, one can take k big enough so that $\Gamma_k(G)$ becomes a connected graph, for example, take $k\geqslant d(G)+\bar{d}(G)$, where $d(G)$ is the minimal number of generators for G and $\bar{d}(G)$ is the maximal size of the minimal generating set for G. However, it is still unknown that whether $\Gamma_k(G)$ is connected for $k\geqslant 3$ or not when G is a finite simple group. Note that $d(G)\leqslant 2$ for finite simple groups. Pak proved in [44] that, for a fixed $k\geqslant 3$, we have large connected components for large simple groups G, that is, there exists connected components $\Gamma'_k(G)\subset\Gamma_k(G)$ such that

$$\frac{|\Gamma'_k(G)|}{|\Gamma_k(G)|}\to 1 \quad \text{as} \quad |G|\to\infty.$$

The product replacement algorithm was implemented in GAP and it has very successful practical performance, see [22] for more details.

1.3 A plan for the recognition of black box groups

As discussed in the previous section, the existing constructive recognition algorithms for classical groups depend on the discrete logarithm problem and the consructive recognition of $\mathrm{SL}_2(q)$. Moreover these algorithms depend slightly on the type of the input group [15, 16, 17, 34]. Following this observation, we will present an alternative uniform approach for recognizing all the simple groups of Lie type which follows the computational version of the classification of the finite simple groups. Similar to the inductive argument on centralizers of involutions which plays a crucial role in the classification project, our approach is based on a recursive construction of the centralizers of involutions in black box groups [13, 14].

We propose the following plan for the recognition of the black box finite simple groups of Lie type of known odd characteristic.

> Construct a list of subgroups which are root $\mathrm{SL}_2(q)$-subgroups in G corresponding to the nodes in the extended Dynkin diagram of G.

Observe that this procedure determines the isomorphism type of G uniquely, see Table 2.1 on page 15. Note that this procedure is not a constructive recognition of G. However, it allows us to construct all *subsystem subgroups* of G, which can be read from the extended Dynkin diagram. To define a subsystem subgroup and make the arguments uniform, we introduce the following definition. Let G be a untwisted group of Lie type of rank n, then we call a maximal split torus, which is of order $(q-1)^n$, a *maximal standard torus*. For the twisted groups, except for $\mathrm{P}\Omega^-_{2n}(q)$, n even, and ${}^3D_4(q)$, we define a maximal standard torus as a maximal torus of order $(q+1)^n$ where n is the Lie rank of the corresponding simple algebraic group. For $G = \mathrm{P}\Omega^-_{2n}(q)$, n even, or ${}^3D_4(q)$, tori of orders $(q+1)^{n-1}(q-1)$ or $(q-1)(q^3-1)$ will be called maximal standard tori of G respectively. Except for Suzuki-Ree groups, a "subsystem subgroup" of a finite simple group G of Lie type is a quasi-simple subgroup of G normalized by a maximal standard torus. In this setting, it turns out that the long root $\mathrm{SL}_2(q)$-subgroups are subsystem subgroups of finite simple groups of Lie type of odd characteristic.

Note that this procedure is a computational version of Aschbacher's "Classical Involution Theorem" [3]. Aschbacher's characterization of Chevalley groups over fields of odd order is based on the study of "2-components"

in the centralizers of involutions. Recall that a 2-*component* of a group G is a perfect subnormal subgroup L such that $L/O(L)$ is quasi-simple where $O(L)$ is the maximal normal subgroup of L of odd order and *solvable* 2-*component* of G is a subnormal subgroup L of G with $O(L) = O(G)$ and $L/O(L) = (\mathrm{P})\mathrm{SL}_2(3)$. Aschbacher's Classical Involution Theorem reads:

> *Let G be a finite group the generalized Fitting subgroup $F^*(G)$ simple. Let z be an involution in G and K a 2-component or solvable 2-component of $C_G(z)$ of 2-rank 1 containing z. Then $F^*(G)$ is a Chevalley group of odd characteristic or M_{11}.*

The involutions satisfying the hypothesis of the above theorem are called *classical involutions*. Taking the "Classical Involution Theorem" as a model, we extend our setting to the black box groups X where $X/O_p(X)$ is a finite simple group of Lie type of odd characteristic. Observe that an involution $i \in X$ belongs to a 2-component or solvable 2-component of $C_X(i)$ of 2-rank 1 if and only if $\bar{i} \in X/O_p(X)$ belongs to a 2-component or solvable 2-component of $C_{X/O_p(X)}(\bar{i})$ of 2-rank 1 since p is odd. Hence Aschbacher's characterization fits into this setting, and we propose the following project for the recognition of black box group X where $X/O_p(X)$ is a finite simple group of Lie type of known odd characteristic p.

> **Procedure 1:** Construct a subgroup K where $K/O_p(K)$ is a long root $\mathrm{SL}_2(q)$-subgroup in $X/O_p(X)$.
>
> **Procedure 2:** Determine whether $O_p(X) \neq 1$.
>
> **Procedure 3:** Construct subgroups K where $K/O_p(K)$ is root $\mathrm{SL}_2(q)$-subgroups in G corresponding to the nodes in the extended Dynkin diagram of G.

In this thesis Procedure 1 is completed in Chapter 4, Procedure 2 is carried out in Chapter 5 for the groups X where $X/O_p(X)$ is a classical group or unisingular group and we completed Procedure 3 in Chapter 6 for the groups $\mathrm{PSL}_n(q)$ and $\mathrm{PSU}_n(q)$.

1.4 Statements of results

In this section we summarize the results presented in this thesis. Let X denote a black box group with the property that $X/O_p(X)$ is isomorphic to

a finite simple group of Lie type defined over a field $\mathbb{F}_q$ of odd characteristic p, $q = p^k$ for some $k \geqslant 1$.

We are mainly interested in the case that the size of the base field is large. Note that our algorithms work for the groups over small fields as well, provided that solvable 2-components do not occur in the centralizers of involutions or equivalently when $q > 3$. However there are better algorithms where $X/O_p(X)$ can be recognized constructively when the size of the underlying field is small [34].

In our algorithms we assume that the characteristic p of the underlying field is given as an input. In this thesis, we do not attempt to find the exact orders of the elements as the computation of the order of an element in a black box group is not a polynomial time task in the input length unless one assumes additional information, for example, the set of primes dividing the order of the input group. Instead, we work with a milder assumption that a computationally feasible global exponent E for X, that is, a reasonably sized natural number E such that $x^E = 1$ for all $x \in X$ is given as an input. We do not assume that we know the exact factorization of E into primes since then we can compute the orders of the elements. Note that having such an exponent for a black box group, we can immediately conclude, in certain cases, that whether X is isomorphic to a known finite group G, for example, if we find an element $x \in X$ satisfying $x^{|G|} \neq 1$ then, clearly, $X \ncong G$. To check whether $x^{|G|} \neq 1$, we use square-and-multiply method, which involves only $O(\log |G|)$ multiplications in the group.

The main result is the following.

Theorem 1.1. *Let X be a black box group and assume that $\bar{X} = X/O_p(X)$ is isomorphic to a finite simple group of Lie type defined over a field of known odd size $q = p^k > 3$ for some $k \geqslant 1$. Assume also that $\bar{X} \neq \mathrm{PSL}_2(q)$ and $\bar{X} \neq {}^2G_2(q)$, then there is a one sided Monte–Carlo polynomial time algorithm which finds the size of the underlying field and constructs a subgroup K such that $K/O_p(K)$ is a long root $\mathrm{SL}_2(q)$-subgroup in $\bar{X}$.*

If $X/O_p(X)$ is a Lie type group defined over a field of odd characteristic p with non-trivial center, then we can find $Z(X)$ by a Monte–Carlo polynomial time algorithm in [10]. Therefore the algorithm in Theorem 1.1 can be extended to the quasi-simple groups of Lie type over a field of odd size $q > 3$.

In the case of a black box group X where $\bar{X} = X/O_p(X)$ is isomorphic to $\mathrm{PSL}_2(q)$ or ${}^2G_2(q)$, there is no subgroup in $\bar{X}$ isomorphic to $\mathrm{SL}_2(q)$. Therefore it is natural to exclude these groups in Theorem 1.1. The following theorem

allows us to decide whether given a subgroup is a long root $\mathrm{SL}_2(q)$-subgroup in a finite simple group of Lie type defined over a field of odd size $q > 3$.

Theorem 1.2. *Let K be a subgroup in a finite simple black box group G of Lie type defined over a field of odd size $q > 3$ isomorphic to $(\mathrm{P})\mathrm{SL}_2(q^k)$ for some $k \geqslant 1$. Then there is a one sided Monte–Carlo polynomial time algorithm which decides whether K is a long root $\mathrm{SL}_2(q)$-subgroup in G.*

Theorem 1.1 yields some further algorithms answering several questions in black box group theory. The first of these is a Monte–Carlo algorithm which determines whether $O_p(X) \neq 1$ in polynomial time answering a well-known question of Babai-Shalev [10]. We will prove the following theorem.

Theorem 1.3. *Let X be a black box group with the property that $X/O_p(X)$ is a simple classical group of odd characteristic p. Then we can determine, in polynomial time, whether $O_p(X) \neq 1$, and, if $O_p(X) \neq 1$, we can find a non-trivial element from $O_p(X)$.*

As an another application of Theorem 1.1 we present a probabilistic recognition algorithm for classical groups.

Theorem 1.4. *Let G be a black box classical group defined over a field of odd size $q > 3$, and rank $n \geqslant 3$. Then there is a one sided Monte–Carlo polynomial time algorithm which determines the type of the group G.*

An immediate corollary to Theorem 1.4 is an alternative algorithm distinguishing symplectic groups $\mathrm{PSp}_{2n}(q)$ from orthogonal groups $\Omega_{2n+1}(q)$. Such an algorithm was first proposed by Altseimer and Borovik in [1] using again centralizers of involutions and conjugacy classes in these groups but their method was completely different than the one presented in Theorem 1.4.

In the following theorem we present the Curtis-Tits system for the groups $(\mathrm{P})\mathrm{SL}_n(q)$ and $(\mathrm{P})\mathrm{SU}_n(q)$.

Theorem 1.5. *Let G be a black box group known to be isomorphic to $(\mathrm{P})\mathrm{SL}_n(q)$ or $(\mathrm{P})\mathrm{SU}_n(q)$, $n \geqslant 3$ $q \geqslant 5$ odd. Then there exists a polynomial-time Monte-Carlo algorithm which constructs all long root $\mathrm{SL}_2(q)$-subgroups corresponding to the nodes in the extended Dynkin diagram of $(\mathrm{P})\mathrm{SL}_n(q)$. In particular, the algorithm determines the isomorphism type of the given group.*

The algorithms presented in this thesis have been implemented extensively in the computer algebra system GAP [27] and no technical difficulties have appeared.

Chapter 2

Finite groups of Lie type

In this chapter we collect some basic properties of finite simple groups of Lie type which will be needed in the subsequent chapters. The standard references for a detailed discussion are [19], [20], [25, Chapter 2], [47]. We assume some well-known facts about linear algebraic groups which can be found in [25, Chapter 1] or in [30].

Throughout this chapter $\bar{G}$ denotes a simple algebraic group over an algebrically closed field K of characteristic p, $\bar{T}$ a maximal torus of $\bar{G}$, Σ the $\bar{T}$-root system of $\bar{G}$, Π a fundamental system in Σ, Σ^+ the corresponding positive system and $\bar{B}$ the corresponding Borel subgroup of $\bar{G}$ containing $\bar{T}$. Thus $\bar{B} = \bar{U}\bar{T}$ where $\bar{U} = R_u(\bar{B})$, unipotent radical of $\bar{B}$. We also set $\bar{N} = N_{\bar{G}}(\bar{T})$ and $W = \bar{N}/\bar{T}$.

2.1 Frobenious endomorphisms

It is well known that an algebraic group $\bar{G}$ over an algebraically closed field K of characteristic p can be embedded into $\mathrm{GL}_n(K)$ for some $n \in \mathbb{N}$. Let $q = p^l$, $l \geqslant 1$ and σ_q be the map of $\mathrm{GL}_n(K)$ into itself given by

$$a_{ij} \mapsto (a_{ij}^q).$$

Then σ_q is an endomorphism of $\mathrm{GL}_n(K)$.

A homomorphism $\sigma : \bar{G} \to \bar{G}$ is called a *standard Frobenious homomorphism* if

$$i(\sigma(g)) = \sigma_q(i(g))$$

where i is an embedding of $\bar{G}$ into $\mathrm{GL}_n(K)$ for some n and q is some power of p. A homomorphism $\sigma : \bar{G} \to \bar{G}$ is called a *Frobenius homomorphism* if some power of σ is a standard Frobenious homomorphism.

Let σ be a Frobenius homomorphism of $\bar{G}$ and define

$$\bar{G}_\sigma = \{g \in \bar{G} \mid \sigma(g) = g\}.$$

It is clear that $\bar{G}_\sigma$ is a finite subgroup of $\bar{G}$.

The following theorem, referred as Lang–Steinberg Theorem, is the key result to pass to finite groups from algebraic groups.

Fact 2.1. **[Theorem 10.1 in [47]]** *Let $\bar{G}$ be a connected linear algebraic group and σ be a surjective homomorphism of $\bar{G}$ onto $\bar{G}$. If $\bar{G}_\sigma$ is finite, then the map*

$$\begin{array}{rcl} \bar{G} & \to & \bar{G} \\ g & \mapsto & g\sigma(g^{-1}) \end{array}$$

is surjective.

We need the following definition to study the structural properties of the finite groups $\bar{G}_\sigma$.

Definition 2.2. *Let G be a group and σ be an endomorphism of G. Then $H^1(\sigma, G)$ is the set of equivalence classes of G under the relation $\sim$ defined by*

$$x \sim y \text{ if and only if } y = gx\sigma(g^{-1}) \text{ for some } g \in G.$$

If $x, y \in G$ are equivalent under this equivalence relation we say that they are σ-conjugate.

Fact 2.3. **[Theorem 2.1.4 in [25]]** *Let $\bar{G}$ be a connected simple algebraic group and σ a Frobenious endomorphism of $\bar{G}$. Let $\bar{H}$ be a closed σ-invariant subgroup of $\bar{G}$. Then the canonical mapping $\bar{H} \to \bar{H}/\bar{H}^\circ$ induces a bijection*

$$H^1(\sigma, \bar{H}) \to H^1(\sigma, \bar{H}/\bar{H}^\circ).$$

The following consequence of Lang-Steinberg Theorem plays a crucial role in the study of finite groups.

Fact 2.4. **[Theorem 2.1.5 in [25]]** *Let $\bar{G}$ be a simple algebraic group and σ a Frobenious endomorphism of $\bar{G}$. Suppose that the semidirect product $\bar{G} \rtimes \langle\sigma\rangle$ acts on a non-empty set Ω in such a way that $\bar{G}$ acts transitively and the stabilizer $\bar{G}_\omega$ in $\bar{G}$ of some $\omega \in \Omega$ is closed. Then $\Omega_\sigma = \{\omega \in \Omega \mid \omega^\sigma = \omega\} \neq \emptyset$. Furthermore, if $\omega \in \Omega_\sigma$, then the set of $\bar{G}_\sigma$-orbits on the stabilizer Ω_σ is in one-to-one correspondence with $H^1(\sigma, \bar{G}_\omega/\bar{G}_\omega^\circ)$. In particular, if $\bar{G}_w$ is connected, then $\bar{G}_\sigma$ acts transitively on Ω_σ.*

An immediate consequence of Fact 2.4 is the following.

Fact 2.5. [Theorem 2.1.6 in [25]] *Let $\bar{G}$ be a connected simple algebraic group and σ a Frobenious endomorphism of $\bar{G}$. Then*

1. *There exist a maximal torus $\bar{T}$ and Borel subgroup $\bar{B}$ of $\bar{G}$ which are σ-invariant and $\bar{T} \leqslant \bar{B}$. Moreover $\bar{G}_\sigma$ permutes transitively the set of all such pairs $(\bar{T}, \bar{B})$.*

2. *There are $\mid H^1(\sigma, N_{\bar{G}}(\bar{T})/\bar{T}) \mid$ classes of σ-invariant maximal tori under conjugation by $\bar{G}_\sigma$ where $\bar{T}$ is a σ-invariant maximal torus.*

It is important to observe that Frobenious endomorphisms give rise to a permutation on the set of fundamental roots of $\bar{G}$. Let σ be a Frobenious endomorphism of $\bar{G}$, $\bar{B}$ be a σ-invariant Borel subgroup of $\bar{G}$ and $\bar{T}$ a σ-invariant maximal torus of $\bar{G}$ contained in $\bar{B}$. Now, $\bar{U} = R_u(\bar{B})$ is also σ-invariant and the root subgroups X_α, $\alpha \in \Sigma^+$, are permuted by σ, that is, σ determines a permutation ρ on the positive roots, $\sigma(X_\alpha) = X_{\rho\alpha}$. Indeed, ρ is a permutation on the set of fundamental roots, $\rho(\Pi) = \Pi$.

2.2 Finite groups of Lie type

We follow the same notation and terminology in [25] to construct finite groups from algebraic groups.

Definition 2.6. *A σ-setup over an algebraically closed field $\bar{\mathbb{F}}_p$ is a pair $(\bar{G}, \sigma)$ such that $\bar{G}$ is a simple algebraic group over $\bar{\mathbb{F}}_p$ and σ is a Frobenious endomorphism of $\bar{G}$. A σ-setup for a finite group G is a σ-setup $(\bar{G}, \sigma)$ over $\bar{\mathbb{F}}_p$ for some prime p such that G is isomorphic to the subgroup $O^{p'}(C_{\bar{G}}(\sigma))$ of $C_{\bar{G}}(\sigma)$ generated by all its p-elements.*

In the rest of this chapter G will denote a finite group possessing a σ-setup $(\bar{G}, \sigma)$ where $\bar{G}$ is a simple algebraic group over $\bar{\mathbb{F}}_p$. We denote the set consisting of all such groups by $\mathcal{L}ie(p)$.

For any simple algebraic group $\bar{G}$ with a root system Σ, there exist simple algebraic groups $\bar{G}_u$ and $\bar{G}_a$, *unique* up to isomorphism of algebraic groups, with Σ as their root system. Moreover, there exist isogenies

$$\bar{G}_u \to \bar{G} \to \bar{G}_a.$$

Recall that an *isogeny* of algebraic groups is a surjective morphism with finite kernel. The groups $\bar{G}_u$ and $\bar{G}_a$ are called the *universal* and *adjoint* versions of $\bar{G}$ respectively.

Fact 2.7. [**Theorem 2.1.2 (e) in [25]**] *Let $\bar{G}$ be a simple algebraic group and σ be a Frobenious endomorphism of $\bar{G}$. Let $\bar{G}_u \to \bar{G} \to \bar{G}_a$ be isogenies of $\bar{G}$. Then σ lifts to a Frobenious endomorphism σ_u of $\bar{G}_u$ and induces a Frobenious endomorphism σ_a of $\bar{G}_a$.*

Let $(\bar{G}, \sigma)$ be a σ-setup for G. Then we have Frobenious endomorphisms σ_u and σ_a for $\bar{G}_u$ and $\bar{G}_a$, respectively, as in Fact 2.7 by considering the isogenies $\bar{G}_u \to \bar{G} \to \bar{G}_a$ which lead to the σ-setups $(\bar{G}_u, \sigma_u)$ and $(\bar{G}_a, \sigma_a)$ for the groups denoted G_u and G_a, respectively. Hence we have finite groups $G_u = O^{p'}(C_{\bar{G}_u}(\sigma_u))$ and $G_a = O^{p'}(C_{\bar{G}_a}(\sigma_a))$. The properties of the groups G_u and G_a are summarized in the following fact.

Fact 2.8. [**Theorem 2.2.6 in [25]**] *Let $(\bar{G}, \sigma)$ be a σ-setup for G and let G_u and G_a be universal and adjoint versions of G, respectively. Then*

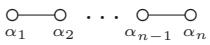
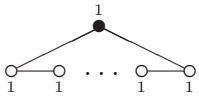
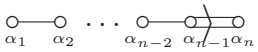
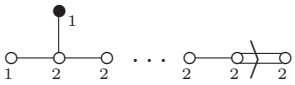
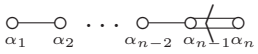
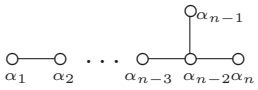
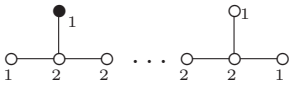
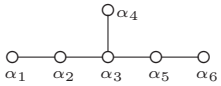
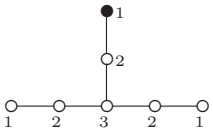
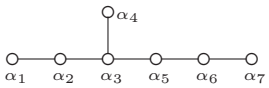
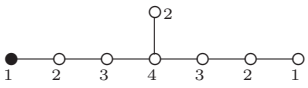
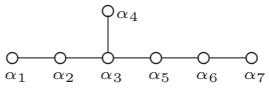
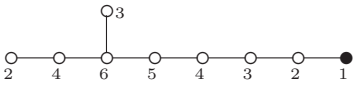
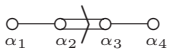
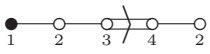
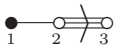
1. *The groups G_u and G_a are unique up to isomorphism.*
2. *There are surjective homomorphisms $G_u \to G \to G_a$ whose kernels are central. In particular, if G is simple, then $G \cong G_a$.*
3. *$Z(G_a) = 1$ and $G/Z(G) \cong G_u/Z(G_u) \cong G_a$.*
4. *The versions of G are the groups G_u/Z where Z ranges over all subgroups of $Z(G_u)$.*
5. *If $(\bar{G}, \sigma)$ is a σ-setup for G with $\bar{G}$ universal, then $\bar{G}_\sigma$ is generated by its p-elements so that $G \cong \bar{G}_\sigma$.*
6. *If $(\bar{G}, \sigma)$ is a σ-setup for G, then $\bar{G}_\sigma = G\bar{T}_\sigma$ for any σ-invariant maximal torus $\bar{T}$ of $\bar{G}$.*

Recall that Frobenious endomorphisms act on the Dynkin diagrams and the Dynkin diagram of the finite groups of Lie type is not necessarily same as the Dynkin diagram of the corresponding algebraic group.

The isomorphism type of G is uniquely determined by

- the Dynkin diagram,

Table 2.1: Dynkin diagrams of simple algebraic groups

	Dynkin diagram	Extended Dynkin diagram
A_n		
B_n		
C_n		
D_n		
E_6		
E_7		
E_8		
F_4		
G_2		

- the symmetry of the Dynkin diagram, discussed at the end of Section 2.1,
- the version of $\bar{G}$, and
- the number q.

We have the following classes of finite groups of Lie type.

• The groups G whose Dynkin diagrams are same as the Dynkin diagrams of $\bar{G}$ are called the *untwisted* groups of Lie type. These groups are $A_n(q)$, $B_n(q)$, $C_n(q)$, $D_n(q)$, $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, $G_2(q)$.

• The groups having a Dynkin diagram with a non-trivial symmetry which does not interchange the length of the roots are called the *twisted* groups of Lie type. We denote these groups by ${}^2A_n(q)$, ${}^2D_n(q)$, ${}^3D_4(q)$, ${}^2E_6(q)$ where the Frobenious endomorphism induces a field automorphism of order 2 on $\mathbb{F}_{q^2}$.

• The groups having a Dynkin diagram with a symmetry which interchanges the long roots to short roots and preserves the angle between roots are called the *Suzuki-Ree* groups. These are ${}^2B_2(2^{a+1/2})$, ${}^2F_4(2^{a+1/2})$, ${}^2G_2(3^{a+1/2})$.

$A_n(q)$: If G is universal, then $G \cong \mathrm{SL}_{n+1}(q)$. If G is adjoint then $G \cong \mathrm{PSL}_{n+1}(q)$. The number q can take any value which is a power of p.

$B_n(q)$: If G is universal, then $G \cong Spin_{2n+1}(q)$, and if G is adjoint, then $G \cong \Omega_{2n+1}(q)$ corresponding to a non-degenerate quadratic form over $\mathbb{F}_q$ of maximal Witt index n. The number q can take any value which is a power of p.

$C_n(q)$: If G is universal, then $G \cong \mathrm{Sp}_{2n}(q)$. If G is adjoint then $G \cong \mathrm{PSp}_{2n}(q)$. The number q can take any value which is a power of p.

$D_n(q)$: If G is universal, then $G \cong Spin^+_{2n}(q)$, and if G is adjoint, then $G \cong \mathrm{P}\Omega^+_{2n}(q)$ corresponding to a non-degenerate quadratic form over $\mathbb{F}_q$ of maximal Witt index n. The number q can take any value which is a power of p.

${}^2A_n(q)$: If G is universal, then $G \cong \mathrm{SU}_{n+1}(q)$. If G is adjoint then $G \cong \mathrm{PSU}_{n+1}(q)$.

${}^2D_n(q)$: If G is universal, then $G \cong Spin^-_{2n}(q)$, and if G is adjoint, then $\mathrm{P}\Omega^-_{2n}(q)$ corresponding to a non-degenerate quadratic form of maximal Witt index $n-1$ over $\mathbb{F}_q$ and Witt index n over $\mathbb{F}_{q^2}$.

${}^3D_4(q)$: In this case $G_u \cong G_a$.

$E_6(q)$: There are two non-isomorphic possibilities G_u and G_a, and $Z(G_u) \cong Z_{(3,q-1)}$.

$E_7(q)$: There are two non-isomorphic possibilities G_u and G_a, and $Z(G_u) \cong Z_{(2,q-1)}$.

$E_8(q)$, $F_4(q)$, $G_2(q)$: In these types $G_u \cong G_a$.

${}^2B_2(q)$, ${}^2F_4(q)$: In these types $G_u \cong G_a$ and $p = 2$ with $q^2 = 2^{2k+1}$ for some $k \geqslant 0$.

${}^2G_2(q)$: In this type $G_u \cong G_a$ and $p = 3$ with $q^2 = 3^{2k+1}$ for some $k \geqslant 0$.

Fact 2.9. [**Theorem 2.2.7 in [25]**] *Let $G \in \mathcal{L}ie(p)$. If G is adjoint, then G is a non-abelian finite simple group with the following exceptions: $G = A_1(2), A_1(3),^2 A_2(2), B_2(2),^2 B_2(2),^2 F_4(2), G_2(2),^2 G_2(3)$. Moreover, G is quasisimple with the same exceptions in all versions.*

Fact 2.10. [**Theorem 2.2.10 in [25]**] *Among the finite simple groups of Lie type and alternating groups A_n, $n \geqslant 5$, the complete list of isomorphisms is given as follows.*

1. *q arbitrary:*
   - $\mathrm{PSL}_2(q) \cong \mathrm{PSp}_2(q) \cong \mathrm{P}\Omega_3(q) \cong \mathrm{PSU}_2(q)$,
   - $\mathrm{PSp}_4(q) \cong \mathrm{P}\Omega_5(q)$,
   - $\mathrm{P}\Omega_4^+(q) \cong \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q)$,
   - $\mathrm{P}\Omega_4^-(q) \cong \mathrm{PSL}_2(q^2)$,
   - $\mathrm{P}\Omega_6^+(q) \cong \mathrm{PSL}_4(q)$,
   - $\mathrm{P}\Omega_6^-(q) \cong \mathrm{PSU}_4(q)$.
2. *q even:* $\mathrm{PSp}_{2n}(q) \cong \mathrm{P}\Omega_{2n+1}(q)$.
3. $\mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5) \cong A_5$, $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$, $\mathrm{PSL}_2(9) \cong A_6$, $\mathrm{PSL}_4(2) \cong A_8$, $\mathrm{PSU}_4(2) \cong \mathrm{P}\Omega_5(3)$.

The orders of finite groups of Lie type will be useful in the sequel and is given in Table 2.2. We use the following notation in Table 2.2. Let $\varepsilon = \pm$, then we write $A_n^+(q)$, $D_n^+(q)$ etc. to denote the untwisted types and $A_n^-(q)$, $D_n^-(q)$ etc. to denote the twisted types.

Table 2.2: Orders of finite groups of Lie type

G_u	Order of G_u
$A_n^\varepsilon(q)$	$q^{n(n+1)/2}\prod_{i=1}^{n}(q^{i+1}-\varepsilon^{i+1})$
$B_n(q)$	$q^{n^2}\prod_{i=1}^{n}(q^{2i}-1)$
$C_n(q)$	$q^{n^2}\prod_{i=1}^{n}(q^{2i}-1)$
$D_n^\varepsilon(q)$	$q^{n(n-1)}(q^n-\varepsilon)\prod_{i=1}^{n-1}(q^{2i}-1)$
${}^3D_4(q)$	$q^{12}(q^2-1)(q^6-1)(q^8+q^4+1)$
$E_6^\varepsilon(q)$	$q^{36}(q^2-1)(q^5-\varepsilon)(q^6-1)(q^8-1)(q^9-\varepsilon)(q^{12}-1)$
$E_7(q)$	$q^{63}(q^2-1)(q^6-1)(q^8-1)(q^{10}-1)(q^{12}-1)(q^{14}-1)(q^{18}-1)$
$E_8(q)$	$q^{120}(q^2-1)(q^8-1)(q^{12}-1)(q^{14}-1)(q^{18}-1)$ $\cdot(q^{20}-1)(q^{24}-1)(q^{30}-1)$
$F_4^\varepsilon(q)$	$q^{24}(q^2-1)(q^6-\varepsilon)(q^8-1)(q^{12}-\varepsilon)$
$G_2^\varepsilon(q)$	$q^6(q^6-\varepsilon)(q^2-1)$

2.3 Root systems

In this section we review the construction of the root systems for a finite group $G \in \mathcal{L}ie(p)$. Let Σ be a $\bar{T}$-root system of $\bar{G}$ for a maximal torus $\bar{T}$, Σ^+ corresponding positive sysem, $\bar{B}$ the corresponding Borel subgroup of $\bar{G}$ containing $\bar{T}$ and W the Weyl group of $\bar{G}$. We have seen that the Frobenious endomorphism σ of $\bar{G}$ determines a permutation on the set of fundamental roots of $\bar{G}$ at the end of Section 2.1. It turns out that this permutation gives rise to a symmetry ρ of the Dynkin diagram of $\bar{G}$ in the sense that the number of bonds joining the nodes is left invariant under ρ. Hence the order

of ρ is 1, 2 or 3 by an immediate observation on the Dynkin diagrams, see Table 2.1.

Let $V = \mathbb{R}\Sigma$ be the Euclidean space spanned by Σ and τ be the isometry of V extending the isometry ρ of Π. We set

$$\widetilde{V} = C_V(\tau) \text{ and } \widetilde{W} = C_W(\tau).$$

Let $\tilde{v}$ denote the orthogonal projection of v onto the subspace $\tilde{V}$. Then $\tilde{v}$ is the average of the vectors in the orbit of v under τ and $\widetilde{\Sigma} = \{\tilde{\alpha} \mid \alpha \in \Sigma\}$ is an orthogonal projection of Σ on $\widetilde{V}$.

Let $\widehat{\Sigma}$ be the set of equivalence classes of $\widetilde{\Sigma}$ under the relation $\sim$ on $\widetilde{\Sigma}$ defined by

$$\tilde{v}_1 \sim \tilde{v}_2 \text{ if and only if } \tilde{v}_1 = c\tilde{v}_2 \text{ for some } c > 0.$$

Thus we have the following mappings.

$$\begin{array}{ccccc} \Sigma & \to & \widetilde{\Sigma} & \to & \widehat{\Sigma} \\ \alpha & \mapsto & \tilde{\alpha} & \mapsto & \hat{\alpha} \end{array}$$

It turns out that the finite subset $\widetilde{\Sigma}$ of $\widetilde{V}$ is a root system, not necessarily reduced, and it is called the *twisted root system* of G. Note that if G is untwisted, then $\tau = 1$, and if G is twisted or Suzuki-Ree group, then the order of the isometry τ is greater than 1.

Remark 2.11. *We note the three possibilities*

1. $\Sigma = \widetilde{\Sigma} = \widehat{\Sigma}$, *if* G *is untwisted.*
2. $\Sigma \neq \widetilde{\Sigma} = \widehat{\Sigma}$, *if* G *is twisted except* ${}^2A_{2n}(q)$.
3. $\Sigma \neq \widetilde{\Sigma} \neq \widehat{\Sigma}$, *if* $G = {}^2A_{2n}(q)$ *or Suzuki-Ree groups.*

Fact 2.12. [Theorem 2.3.4(a) in [25]] *Let* $G \in \mathcal{L}ie(p)$, $N = \bar{N} \cap G$, $H = \bar{T} \cap G$, $B = \bar{B} \cap G$, $U = \bar{U} \cap G$ *with the notation fixed in the beginning of the chapter, we have*

(1) $N\bar{T}/\bar{T} \cong \widetilde{W}$. *In particular* $N/H \cong \widetilde{W}$.

(2) B *is the semidirect product of* U *by* H *and* $U = O_p(B)$, *the maximal normal* p*-subgroup of* B.

Let $\Pi = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a fundamental system for $\bar{G}$ where the labelling of the roots are as in the left column of Table 2.1. Then the explicit description of the root systems and Weyl groups of twisted groups of Lie type are as follows.

- ${}^2A_n(q)$:

  If $n = 2k + 1$, then

  $$\widetilde{\Pi} = \{\frac{1}{2}(\alpha_1 + \alpha_{2k+1}), \frac{1}{2}(\alpha_2 + \alpha_{2k}), \ldots, \frac{1}{2}(\alpha_k + \alpha_{k+2}), \alpha_{k+1}\},$$

  and its Weyl group is isomorphic to the Weyl group of type C_{k+1}.

  If $n = 2k$, then

  $$\widetilde{\Pi} = \{\frac{1}{2}(\alpha_1 + \alpha_{2k}), \frac{1}{2}(\alpha_2 + \alpha_{2k-1}), \ldots, \frac{1}{2}(\alpha_k + \alpha_{k+1})\},$$

  and its Weyl group is isomorphic to the Weyl group of type B_{k+1}.

- ${}^2D_n(q)$:

  $$\widetilde{\Pi} = \{\alpha_1, \alpha_2, \ldots, \alpha_{n-2}, \frac{1}{2}(\alpha_{n-1} + \alpha_n)\}.$$

  The Weyl group is isomorphic to the Weyl group of type B_{n-1}.

- ${}^2E_6(q)$:

  $$\widetilde{\Pi} = \{\frac{1}{2}(\alpha_1 + \alpha_6), \frac{1}{2}(\alpha_2 + \alpha_5), \alpha_3, \alpha_4\}.$$

  The Weyl group is isomorphic to the Weyl group of type F_4.

- ${}^3D_4(q)$:

  $$\widetilde{\Pi} = \{\alpha_2, \frac{1}{3}(\alpha_1 + \alpha_3 + \alpha_4)\}.$$

  The Weyl group is isomorphic to the Weyl group of type G_2.

2.4 Root subgroups

In this section, we review the construction of the root subgroups for the finite groups $G \in \mathcal{L}ie(p)$, p odd. Therefore we do not consider the groups ${}^2B_2(2^{a+1/2})$ and ${}^2F_4(2^{a+1/2})$.

For each $\alpha \in \Sigma$, define $\Sigma_{\hat{\alpha}} = \{\beta \in \Sigma \mid \tilde{\beta} = c\tilde{\alpha},\ c > 0\}$, and set

$$\bar{Y}_{\hat{\alpha}} = \prod_{\beta \in \Sigma_{\hat{\alpha}}} \bar{X}_\beta \quad \text{and} \quad X_{\hat{\alpha}} = C_{\bar{Y}_{\hat{\alpha}}}(\sigma).$$

Observe that $\bar{Y}_{\hat{\alpha}}$ is σ-invariant since τ permutes the roots $\beta \in \Sigma_{\hat{\alpha}}$ among themselves where τ is the isometry of $\mathbb{R}\Sigma$ discussed in Section 2.3. Note that the groups $X_{\hat{\alpha}}$ are not necessarily abelian in twisted groups, see Table 2.3.

Table 2.3: The structure of root subgroups in G [25, Table 2.4]. Here E_{q^i} is an elementary abelian group of order q^i.

Type	$\hat{\alpha}$	Remarks
Untwisted	both	$X_{\hat{\alpha}} = X_\alpha \cong E_q$
Twisted except ${}^2A_{2n}(q)$	long	$X_{\hat{\alpha}} \cong E_q$
Twisted except ${}^3D_4(q)$	short	$X_{\hat{\alpha}} \cong E_{q^2}$
${}^3D_4(q)$	short	$X_{\hat{\alpha}} \cong E_{q^3}$
${}^2A_{2n}(q)$	long	$\mid X_{\hat{\alpha}} \mid = q^3$ and $Z(X_{\hat{\alpha}}) \cong E_q$
${}^2G_2(q)$		$\mid X_{\hat{\alpha}} \mid = q^6$ and $Z(X_{\hat{\alpha}}) \cong E_{q^2}$

The root subgroups $X_{\hat{\alpha}}$ satisfy an analogue of the Chevalley Commutator Formula.

Fact 2.13. [Theorem 2.3.7 in [25]] *Let $(\bar{G}, \sigma)$ be a σ-setup for G with $\bar{G}$ simple. Let Σ be the root system for $\bar{G}$. Then*

$$G = \langle X_{\hat{\alpha}} \mid \alpha \in \Sigma \rangle$$

subject to the relations

$$[X_{\hat{\alpha}}, X_{\hat{\beta}}] = \prod_{\{\hat{\gamma} \mid \gamma \in \Sigma\}} X_{\hat{\gamma}}$$

where $\alpha, \beta \in \Sigma$ with $\hat{\alpha} \neq \pm\hat{\beta}$ and $\tilde{\gamma}$ is a linear combination of $\tilde{\alpha}$ and $\tilde{\beta}$ with both coefficients positive.

More details on the structure of the root subgroups can be found in [25, Section 2.4]

Set

$$M_{\hat{\alpha}} = \langle X_{\hat{\alpha}}, X_{-\hat{\alpha}} \rangle, Z_{\hat{\alpha}} = Z(X_{\hat{\alpha}}), K_{\hat{\alpha}} = \langle Z_{\hat{\alpha}}, Z_{-\hat{\alpha}} \rangle,$$

where $Z(X_{\hat{\alpha}})$ is the center of the root subgroup $X_{\hat{\alpha}}$. Then $X_{\hat{\alpha}} \cong Z_{\hat{\alpha}} \cong E_q$, and $K_{\hat{\alpha}} \cong M_{\hat{\alpha}} \cong \mathrm{SL}_2(q)$ except for the groups given in Table 2.4.

The conjugates of the subgroup $K_{\hat{\alpha}}$ are called *long root* $\mathrm{SL}_2(q)$*-subgroups* or *short root* $\mathrm{SL}_2(q)$*-subgroups* if $\hat{\alpha}$ is long or short respectively.

Fact 2.14. [Theorem 14.5 in [3]] *Let $G \in \mathcal{L}ie(p)$, p odd. Let $\hat{\alpha} \in \widehat{\Sigma}$ be a long root. Then*

(1) $K_{\hat{\alpha}} \cong \mathrm{SL}_2(q)$.

(2) $O^{p'}(N_G(K_{\hat{\alpha}})) = K_{\hat{\alpha}} L_{\hat{\alpha}}$ *where* $[K_{\hat{\alpha}}, L_{\hat{\alpha}}] = 1$ *and* $L_{\hat{\alpha}}$ *is the Levi factor of the parabolic subgroup* $N_G(Z_{\hat{\alpha}})$.

Table 2.4: Short root $\mathrm{SL}_2(q)$-subgroups in G [3, Table 14.4].

G	$\hat{\alpha}$	K_α	M_α
$\mathrm{PSU}_{2n+1}(q)$	long	$\mathrm{SL}_2(q)$	$\mathrm{PSU}_3(q)$
$\mathrm{PSU}_n(q)$	short	$\mathrm{PSL}_2(q^2)$	$\mathrm{PSL}_2(q^2)$
$\Omega_{2n+1}(q)$	short	$\mathrm{PSL}_2(q)$	$\mathrm{PSL}_2(q)$
$\mathrm{P}\Omega^-_{2n}(q)$	short	$\mathrm{PSL}_2(q^2)$	$\mathrm{PSL}_2(q^2)$
${}^2E_6(q)$	short	$\mathrm{SL}_2(q^2)$	$\mathrm{SL}_2(q^2)$
${}^3D_4(q)$	short	$\mathrm{SL}_2(q^3)$	$\mathrm{SL}_2(q^3)$

2.5 Maximal tori

A subgroup of G of the form $G \cap \bar{T}$ for some σ-invariant maximal torus $\bar{T}$ of $\bar{G}$ is called a *maximal torus* of G.

A maximal torus $\bar{T} \leqslant \bar{G}$ is called *σ-split* if it is σ-invariant and lies in a σ-invariant Borel subgroup of $\bar{G}$. By Fact 2.5 (a), there is only one conjugacy class of σ-split maximal tori in $\bar{G}_\sigma$. In general, we have the following.

Lemma 2.15. *The set of G-orbits on the set of σ-invariant maximal tori of $\bar{G}$ is in bijective correspondence with $H^1(\sigma, W)$.*

Proof. We know, by Fact 2.5, that the there is a bijection between the $\bar{G}_\sigma$-classes of σ-invariant maximal tori and $H^1(\sigma, W)$. If G is universal, then $G = \bar{G}_\sigma$ by Fact 2.8(5) and the result follows. By taking the homomorphic image of G_u, we get the result in general. □

Note that if σ fixes each element of W, which is the case if G is untwisted, then $H^1(\sigma, W)$ corresponds to the set of conjugacy classes of W.

Let S be the set of representatives of G-orbits on the set of σ-invariant maximal tori of $\bar{G}$. Then $S \cap G$ is the set of representatives of maximal tori of G whose elements correspond to elements $w \in W$ and they will be denoted by T_w. We will call these tori maximal tori of G *twisted* by w. Note that if $w \sim w'$ in the sense of Definition 2.2, then T_w and $T_{w'}$ are G-conjugate.

The following lemma is crucial in our computations in the sequel.

Fact 2.16. [Proposition 3.3.5, 3.3.6 in [20]] *Let $\bar{G}$ be a simple algebraic group and $\bar{T}$ be a σ-invariant maximal torus of $\bar{G}$ such that $\bar{T}_\sigma$ corresponds to an element $w \in W$. If q is the number of elements of the base field on which G is defined, then the characteristic polynomial of w evaluated at q gives the order of $\bar{T}_\sigma$. Moreover $|\bar{N}_\sigma/\bar{T}_\sigma| \cong |C_W(w)|$ where $\bar{N} = N_{\bar{G}}(\bar{T})$.*

The characteristic polynomials of $w \in W$ for G are given in [18] and we give here the orders of maximal twisted tori in classical groups G_u.

- $A_n^\varepsilon(q)$:

  Provided that $l_1 + \ldots + l_k = n + 1$, the orders of the maximal tori in G_u are of the form

  $$(q^{l_1} - \varepsilon^{l_1})(q^{l_2} - \varepsilon^{l_2}) \ldots (q^{l_k} - \varepsilon^{l_k})/(q - \varepsilon).$$

- $B_n(q)$, $C_n(q)$:

  The orders of the tori in G_u are of the form

  $$(q^{l_1} - 1) \ldots (q^{l_r} - 1)(q^{m_1} + 1) \ldots (q^{m_s} + 1)$$

  where $(l_1 + \ldots + l_r) + (m_1 + \ldots + m_s) = n$.

- $D_n^{\varepsilon}(q)$:

  The orders of the tori in G_u are of the form

  $$(q^{l_1}-1)\dots(q^{l_r}-1)(q^{m_1}+1)\dots(q^{m_s}+1)$$

  where $(l_1+\ldots+l_r)+(m_1+\ldots+m_s)=n$. If G_u is untwisted, then s is an even integer and if G_u is twisted, then s is an odd integer.

The table for the orders of maximal tori in exceptional goups of Lie type can be found in [18].

2.6 The structure of the centralizers of involutions

In this section we summarize the structure of centralizers of involutions in simple groups of Lie type of odd characteristic.

Fact 2.17. [Theorem 4.2.2 in [25]] *Let $G \in \mathcal{L}ie(p)$, p odd, $i \in G$ an involution, $C = C_G(i)$. Let $L = O^{p'}(C)$ and Z be the kernel of the covering $G_u \to G$. Then there exist a subgroup $T \leqslant C$ such that the following conditions satisfied.*

1. *L is a central product $L = L_1 \cdots L_s$ where $s \geqslant 0$ and $L_k \in \mathcal{L}ie(p)$.*
2. *T is an abelian p'-subgroup normalizing each L_k.*
3. *Setting $C^\circ = LT$, we have C/C° is an elementary abelian 2-subgroup isomorphic to a subgroup of Z.*

We will call the group L in Theorem 2.17 the *semisimple socle* of C. The following easy corollary will be useful in the sequel.

Corollary 2.18. *Let $G \in \mathcal{L}ie(p)$, p odd and the defining field of size $q > 3$. Then $L = C''$, the second derived subgroup of C.*

Proof. By Fact 2.17 (3), C/C° is abelian which implies $C' \leqslant C^\circ = LT$. Now since T is abelian and normalizes L by Fact 2.17 (2), we have $C'' \leqslant (LT)' = L$ as L is quasimple by Fact 2.9 and the result follows. □

Note that if $G = G_u$, then $Z = 1$ implying $C = C^\circ$ and we have $L = C'$.

Passsing to the groups with a non-trivial p-core we have the following.

Corollary 2.19. *Let X be a finite group. Assume that $X/O_p(X)$ is a finite simple group of Lie type over a field of odd size $q > 3$ and i be an involution in X. Then $(C_X(i)/O_p(C_X(i)))''$ is the semisimple socle of $C_X(i)/O_p(C_X(i))$.*

The table of all possible centralizers of involutions in G_a is given in Table 2.5 which is taken from [25]. In Table 2.5 we use the following notation. Let G be a finite group and $Z(G)$ is cyclic. Then we write $\frac{1}{m}G$ to denote the quotient group G/Y where $Y \leqslant Z(G)$ and $|Y| = m$. Note that the center of $G = \mathrm{Spin}^+_{2n}(q)$, n even, is an elementary abelian group of order 4. Therefore $\frac{1}{2}\mathrm{Spin}^+_{2n}(q)$ is not uniquely defined for n even and we define it as follows. There is an involution $z \in Z(G)$ such that $G/\langle z\rangle \cong \mathrm{SO}^+_{2n}(q)$. For the other involutions z_1, $z_2 \in Z(G)\backslash\{z\}$, we have $G/\langle z_1\rangle \cong G/\langle z_2\rangle$ which is not isomorphic to $\mathrm{SO}^+_{2n}(q)$ and we denote these quotient groups as $\frac{1}{2}\mathrm{Spin}^+_{2n}(q)$. Notice that $\frac{1}{2}\mathrm{Spin}^+_{2n}(q)$, $n = 6, 8$, appears as the component in a centralizer of an involution in the groups $E_7(q)$ and $E_8(q)$, see Table 2.5.

We are mostly interested in the involutions in the long root $\mathrm{SL}_2(q)$-subgroups, which are classical involutions by Fact 2.14, and it is worth to give the list of classical involutions and the semisimple socle of their centralizers Table 2.6.

The following two lemmas will be used to check whether a given subgroup isomorphic to $\mathrm{SL}_2(q)$ for some q in G is long root $\mathrm{SL}_2(q)$-subgroup.

Lemma 2.20. *Let K be a long root $\mathrm{SL}_2(q)$-subgroup of G, $q > 3$, and $z \in Z(K)$. Then $K = K^g$ for any $g \in C_G(z)''$.*

Proof. Corollary 2.18 implies that the second derived subgroup $C_G(z)''$ is the semisimple socle of $C_G(z)$. Hence the result follows since K is a component in $C_G(z)$ by Fact 2.14. □

Lemma 2.21. *Let G be a finite simple group of Lie type over a field of size $q > 3$ different from ${}^3D_4(q)$ and $G_2(q)$. Let K be a short root $\mathrm{SL}_2(q)$-subgroup of G and $z \in K$ be an involution. Then there exists $g \in C_G(z)''$ such that $K \neq K^g$.*

Proof. It is clear from Table 2.4 that if G is $\mathrm{PSU}_n(q)$, $\Omega_{2n+1}(q)$ or $\mathrm{P}\Omega^-_{2n}(q)$, then $K \neq K^g$ where $g \in C_G(z)''$.

If G is $F_4(q)$ or ${}^2E_6(q)$, then $C_G(z)''$ is isomorphic to $\mathrm{Spin}_9(q)$ or $\mathrm{Spin}^-_{10}(q)$ respectively [3, 29.7] in which case there exists $g \in C_G(z)''$ such that $K \neq K^g$.

If $G = \mathrm{PSp}_{2n}(q)$, $n \geqslant 3$, then $K \cong \mathrm{SL}_2(q)$ and the underlying vector space for K is a totally isotropic subspace of dimension 2. Therefore $C_V(z)$ has

Table 2.5: Centralizers of involutions in simple groups of Lie type of odd characteristic.

G	conditions	type	$L = O^{p'}(C_G(i))$	$C_{C_G(i)}(L)$
$\mathrm{PSL}_n^\varepsilon(q)$	$2 \leqslant k \leqslant n/2$	t_1	$\mathrm{SL}_{n-1}^\varepsilon(q)$	$q-\varepsilon$
		t_k	$\mathrm{SL}_k^\varepsilon(q) \circ \mathrm{SL}_{n-k}^\varepsilon(q)$	$q-\varepsilon$
	n even	$t'_{n/2}$	$\frac{1}{(n/2,q-\varepsilon)}\mathrm{SL}_{n/2}(q^2)$	$q+\varepsilon$
$\Omega_{2n+1}(q)$ $n \geqslant 2$		t_1	$\Omega_{2n-1}(q)$	$2(q-1)$
		t'_1	$\Omega_{2n-1}(q)$	$2(q+1)$
	$2 \leqslant k < n$	t_k	$\Omega_{2k}^+(q) \times \Omega_{2(n-k)+1}(q)$	2
	$2 \leqslant k < n$	t'_k	$\Omega_{2k}^-(q) \times \Omega_{2(n-k)+1}(q)$	2
		t_n	$\Omega_{2n}^+(q)$	2
		t'_n	$\Omega_{2n}^-(q)$	2
$\mathrm{PSp}_{2n}(q)$ $n \geqslant 2$	$1 \leqslant k \leqslant n/2$	t_k	$\mathrm{Sp}_{2k}(q) \circ_2 \mathrm{Sp}_{2(n-k)}(q)$	2
		t_n	$\frac{1}{(2,n)}\mathrm{SL}_n(q)$	$q-1$
		t'_n	$\frac{1}{(2,n)}\mathrm{SU}_n(q)$	$q+1$
$\mathrm{P}\Omega_{2n}^\varepsilon(q)$ $n \geqslant 4$		t_1	$\Omega_{2n-2}^\varepsilon(q)$	$q-1$
		t'_1	$\Omega_{2n-2}^{-\varepsilon}(q)$	$q+1$
	$2 \leqslant k < n/2$	t_k	$\Omega_{2k}^+(q) \circ_2 \Omega_{2(n-k)}^\varepsilon(q)$	2
	$2 \leqslant k < n/2$	t'_k	$\Omega_{2k}^-(q) \circ_2 \Omega_{2(n-k)}^{-\varepsilon}(q)$	2
	$\mathrm{P}\Omega_{4m}^+(q)$	$t_{n/2}$	$\Omega_m^+(q) \circ_2 \Omega_m^+(q)$	2
	$\mathrm{P}\Omega_{4m}^+(q)$	$t'_{n/2}$	$\Omega_m^-(q) \circ_2 \Omega_m^-(q)$	2
	$\mathrm{P}\Omega_{4m}^+(q)$	t_{n-1}, t_n	$\frac{1}{2}\mathrm{SL}_n(q)$	$q-1$
	$\mathrm{P}\Omega_{4m}^+(q)$	t'_{n-1}, t'_n	$\frac{1}{2}\mathrm{SU}_n(q)$	$q+1$
	$\mathrm{P}\Omega_{4m}^-(q)$	$t_{n/2}$	$\Omega_m^-(q) \times \Omega_m^+(q)$	2
	$\mathrm{P}\Omega_{2(2m+1)}^\varepsilon(q)$	t_n	$\mathrm{SL}_n^\varepsilon(q)$	$q-\varepsilon$
${}^3D_4(q)$		t_2	$\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q^3)$	2
$G_2(q)$		t_1	$\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$	2
${}^2G_2(q)$		t_1	$\mathrm{PSL}_2(q^2)$	2
$F_4(q)$		t_1	$\mathrm{SL}_2(q) \circ_2 \mathrm{Sp}_6(q)$	2
		t_4	$\mathrm{Spin}_9(q)$	2
$E_6^\varepsilon(q)$		t_1	$\mathrm{Spin}_{10}^\varepsilon(q)$	$q-\varepsilon$
		t_2	$\mathrm{SL}_2(q) \circ_2 \frac{1}{(q-\varepsilon,3)}\mathrm{SL}_6^\varepsilon(q)$	2
$E_7(q)$		t_1	$\mathrm{SL}_2(q) \circ_2 \frac{1}{2}\mathrm{Spin}_{12}(q)$	2
		t_4, t'_4	$\frac{1}{(4,q-\varepsilon)}\mathrm{SL}_8^\varepsilon(q)$	2
		t_7, t'_7	$\hat{E}_6^\varepsilon(q)$	$q-\varepsilon$
$E_8(q)$		t_1	$\frac{1}{2}Spin_{16}(q)$	2
		t_8	$\mathrm{SL}_2(q) \circ_2 E_7(q)$	2

Table 2.6: Classical involutions and the semisimple socles in their centralizers.

G	i	L''
$\mathrm{PSL}_n^\varepsilon(q)$	t_2	$\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_{n-2}^\varepsilon(q)$
$\mathrm{PSp}_{2n}(q)$	t_1	$\mathrm{SL}_2(q) \circ_2 \mathrm{Sp}_{2n-2}(q)$
$\Omega_{2n+1}(q)$	t_2	$(\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)) \circ_2 \Omega_{2n-3}(q)$
$\mathrm{P}\Omega_{2n}^\varepsilon(q)$	t_2	$(\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)) \circ_2 \Omega_{2n-4}^\varepsilon(q)$
$G_2(q)$	t_1	$\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$
${}^3D_4(q)$	t_2	$\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q^3)$
$F_4(q)$	t_1	$\mathrm{SL}_2(q) \circ_2 \mathrm{Sp}_6(q)$
$E_6^\varepsilon(q)$	t_2	$\mathrm{SL}_2(q) \circ_2 \frac{1}{(q-\varepsilon,3)}\mathrm{SL}_6^\varepsilon(q)$
$E_7(q)$	t_1	$\mathrm{SL}_2(q) \circ_2 \frac{1}{2}\mathrm{Spin}_{12}(q)$
$E_8(q)$	t_8	$\mathrm{SL}_2(q) \circ_2 E_7(q)$

dimension $2n-4$ or 4 where V is the underlying vector space for $\mathrm{Sp}_{2n}(q)$ which implies that $C_G(z)'' \cong \mathrm{Sp}_4(q) \circ_2 \mathrm{Sp}_{2n-4}(q)$. Thus there exists $g \in C_G(z)''$ such that $K \neq K^g$. □

If $G = {}^3D_4(q)$ or $G_2(q)$, then $C_G(z) = \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q^3)$ or $\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$ respectively as there is only one conjugacy class of involutions in G. Therefore $K = K^g$ for any $g \in C_G(z)''$.

Chapter 3

Centralizers of involtions in black box groups

In this chapter, we present the necessary tools in the recognition of the black box groups by using the centralizers of involutions.

3.1 Construction of $C_G(i)$ in a black box group

In literature, the construction of centralizer of an involution in black box groups were first appeared in [14] and it was used in [1] to distinguish orthogonal groups $\Omega_{2n+1}(q)$ from $\mathrm{PSp}_{2n}(q)$ for odd q. In [13], the idea of using the structure of centralizers of involutions in the black box recognition algorithms is discussed extensively and some results are announced which come out of this approach. We borrow the notation in [13].

Let X be a black box finite group having an exponent $E = 2^k m$ with m odd. Producing an involution in X, we need an element x of even order. Then the last non-identity element in the sequence

$$1 \neq x^m,\ x^{m2},\ x^{m2^2},\ \ldots,\ x^{m2^{k-1}},\ x^{m2^k} = 1$$

will be an involution and will be denoted by $\mathrm{i}(x)$.

We call an element $j \in X$ of order 4 a *pseudo-involution* if it is an involution in $X/Z(X)$ but not in X. Let $Y \leqslant X$, then we call an element $j \in Y$ a *pseudo-involution* in Y if $1 \neq j^2 \in Z(Y)$. We can produce pseudo-involutions in X in a similar manner, that is, we first produce an element of order 4 and check whether j^2 commutes with the generators of X.

Let t be an involution in X and $x \in X$ a random element. Set $z = tt^x$.

- If the order m of z is odd, then consider $y = z^{(m+1)/2}$. Now observe that $yx^{-1} \in C_X(t)$ and denote $\zeta_1^t(x) = yx^{-1}$.

- If z is of even order, then $\mathrm{i}(z) \in C_X(i)$. Denote $\zeta_0^t(x) = \mathrm{i}(z)$.

Here the superscript ^{t} indicates the dependence of the map ζ_k, $k = 0, 1$, on the involution t.

Thus we have a map $\zeta^t = \zeta_0^t \sqcup \zeta_1^t$ defined by

$$\begin{array}{rcl} \zeta^t : X & \longrightarrow & C_X(t) \\ x & \mapsto & \begin{cases} \zeta_1^t(x) = (tt^x)^{(m+1)/2} \cdot x^{-1} & \text{if } o(tt^x) \text{ is odd} \\ \zeta_0^t(x) = \mathrm{i}(tt^x) & \text{if } o(tt^x) \text{ is even.} \end{cases} \end{array}$$

Here $o(x)$ is the order of the element $x \in X$. Note that one can test whether an element $x \in X$ has odd or even order by raising it to the odd part m of the exponent E. If $o(x)$ is odd then $x^{(m+1)/2} = x^{(o(x)+1)/2}$ and if $o(x)$ is even then $x^m \neq 1$. Therefore we can construct $\zeta_0^t(x)$ and $\zeta_1^t(x)$ without knowing the exact order of tt^x.

Observe that if $c \in C_X(t)$, then

$$\begin{array}{rcl} \zeta_1^t(cx) & = & (tt^{cx})^{(m+1)/2} \cdot x^{-1}c^{-1} = (tt^x)^{(m+1)/2} \cdot x^{-1}c^{-1} \\ & = & \zeta_1^t(x) \cdot c^{-1}, \\ \zeta_0^t(xc) & = & \mathrm{i}(t \cdot t^{xc}) = \mathrm{i}(t^c \cdot t^{xc}) = \mathrm{i}((t \cdot t^x)^c) = \mathrm{i}(tt^x)^c \\ & = & \zeta_0^t(x)^c. \end{array}$$

Hence

Fact 3.1. ([13]) *Let X be a finite group and $t \in X$ be an involution. If the elements $x \in X$ are uniformly distributed and independent in X, then*

(a) *the elements $\zeta_1^t(x)$ are uniformly distributed and independent in $C_X(t)$ and*

(b) *the elements $\zeta_0^t(x)$ form a normal subset of involutions in $C_X(t)$.*

Let $S \subset X$. By abuse of notation we denote by $\zeta^t(S)$ the group generated by the image of the subset S under the map ζ^t.

We will use both of the functions ζ_0^t and ζ_1^t in the recursive steps to generate $C_X(t)$. It follows directly from Fact 3.1 that the image of the function ζ_1^t is $C_X(t)$ and the image of ζ_0^t generates a normal subgroup in $C_X(t)$.

Remark 3.2. If the domain of one of the functions ζ_0^t or ζ_1^t is rarely defined in a group X then the other function is defined for almost all $x \in X$. For

example, let $Y = \mathrm{PSL}_2(q)$ and q is a big odd prime power, then almost all elements are regular semisimple and hence belong to a cyclic torus of order $(q \pm 1)/2$. Note that one of the tori has even order and at least $1/2$ of its elements have even order. Therefore the probability that the elements having even order in Y is at least $1/4$, see also Theorem 4.3. All involutions in Y are conjugate and the product of two random involutions is semisimple with probability close to 1. Therefore the product of two random involutions in Y has even order with probability close to $1/4$. In the group $X = Y \times \ldots \times Y$ (n times), one has to do these computations componentwise and therefore the product of two random involutions has odd order with probability close to $1/2^{2n}$. This shows that when n is a big number, then the map ζ_1 is rarely defined and we have to use the map ζ_0. Although the map ζ_1 is much better for the construction of centralizers of involutions, it turns out that the function ζ_0 suffices for our purposes (see Section 3.2).

3.2 The heart of the centralizer

In this section we describe the subgroup generated by the image of the function ζ_0^i for any involution $i \in G$ where G is a finite simple group of Lie type of odd characteristic. Recall that ζ_0^i does not produce uniformly distributed random elements in centralizers of involutions (see Fact 3.1).

Let $i \in G$ be any fixed involution. We define

$$\heartsuit_i(G) = \langle \zeta_0^i(g) \mid g \in G \rangle.$$

We use here the convention that $\zeta_0^i(g) = 1$ if ii^g has odd order. We also assume that if ii^g has even order, then we assume that $\zeta_1^i(g) = 1$.

Lemma 3.3. *Let G be a finite group and $i \in G$ be an involution. Then ζ_0^i does not produce involutions in the coset $iZ(G)$.*

Proof. Let $g \in G$ such that $\zeta_0^i(g) \neq 1$ and consider the dihedral group $D = \langle i, i^g \rangle$. Recall that $\zeta_0^i(g) = \mathrm{i}(ii^g) \in Z(D)$. Therefore, if $\zeta_0^i(g) = iz$ where z is an involution in $Z(G)$ then i commutes with i^g since $z \in Z(G)$. Hence $\zeta_0^i(g) = ii^g = iz$ implying $i^g = z$ and $i = z$ which gives $\zeta_0^i(g) = 1$, a contradiction. □

Lemma 3.4. *Let $G = G_1 \times G_2$ be a direct product of finite groups G_1, G_2 and $i = (i_1, i_2) \in G$ an involution. Then $\heartsuit_i(G) = \heartsuit_{i_1}(G_1) \times \heartsuit_{i_2}(G_2)$.*

Proof. Recall that the image of ζ_0^i belongs to the conjugacy classes of involutions in $C_G(i)$ by Fact 3.1. Since conjugacy classes of involutions in G are direct product of conjugacy classes of G_1 and G_2, result follows. □

Let $j \in G$ be a pseudo-involution. Then we define

$$\zeta_0^j(g) = \mathrm{i}(jj^g),$$

and

$$\zeta_1^j(g) = (jj^g)^{(m+1)/2} \cdot g^{-1}$$

where $g \in G$ and $\mathrm{i}(jj^g)$ is an involution produced from jj^g as in Section 3.1 and m is the order of jj^g. Observe that $\zeta_0^j(g) \in C_G(j)$. Moreover, we define $\heartsuit_j(G)$ similarly for a pseudo-involution $j \in G$.

In our algorithms, we will need the images of ζ_0^j and ζ_1^j for a pseudo-involution $j \in G$ where $G = \mathrm{SL}_2(q)$.

Lemma 3.5. *Let $G = \mathrm{SL}_2(q)$ and $j \in G$ be a pseudo-involution. Then $\heartsuit_j(G) = Z(G)$.*

Proof. The result follows from the observation that G has unique central involution and the image of the function ζ_0^j is a set of involutions in G. □

Lemma 3.6. *Let $G = \mathrm{SL}_2(q)$ and $j \in G$ be a pseudo-involution. Then $\zeta_1^j(G) = N_G(\langle j \rangle)$ and $\zeta_1^j(G)'' = 1$.*

Proof. Recall that if jj^g has odd order m, then $\zeta_1^j(g) = (jj^g)^{(m+1)/2}g^{-1}$. Let $h = (jj^g)^{(m+1)/2}$, then it is straight forward to check that $j^h = j^2j^g$ which implies that $j^{hg^{-1}} = j^3$ since $j^2 \in Z(G)$. Hence $\zeta_1^j(g) \in N_G(\langle j \rangle)$. It is clear from this observation and Fact 3.1 that $\zeta_1^j(G) = N_G(\langle j \rangle)$. Observe that if j belongs to a torus T then $N_G(\langle j \rangle) = N_G(T)$, $C_G(t) = C_G(T) = T$ and $|N_G(T)/C_G(T)| = 2$ which implies that $\zeta_1^j(G)' \leqslant C_G(j)$ and $\zeta_1^j(G)'' = 1$ since $C_G(j)$ is a cyclic group of order $q \pm 1$. □

Lemma 3.7. *Let $G = (\mathrm{P})\mathrm{Sp}_{2n}(q)$, $q > 3$ and i be an involution of type t_1.*

(a) *If $n \geqslant 3$, then $\heartsuit_i(G)' = \mathrm{Sp}_{2n-2}(q)$.*

(b) *If $G = \mathrm{Sp}_4(q)$, then $\heartsuit_i(G) = Z(G)$.*

(c) *If $G = \mathrm{PSp}_4(q)$, then $\heartsuit_i(G) \geqslant E(C_G(i))$ where $E(C_G(i))$ is the semi-simple socle of $C_G(i)$.*

Proof.

(a) Assume first that $G = \mathrm{Sp}_{2n}(q)$. Then $C_G(i) = \mathrm{SL}_2(q) \times \mathrm{Sp}_{2n-2}(q)$. Let $V = V_- \oplus V_+$ be the decomposition of the corresponding vector space where $V_\pm$ are the eigenspaces of i for the eigenvalues ± 1. Then the dimension of V_- is 2 or $2n-2$. We can assume that $\dim V_- = 2$, the other case is analogous. It is clear that the dimension of the eigenspace of the involution $\zeta_0^i(g)$ for any $g \in G$ and for the eigenvalue -1 is at most 4. Therefore the image of ζ_0^i contains non-central involutions in $\mathrm{Sp}_{2n-2}(q)$ since $n \geqslant 3$. Hence $\heartsuit_i(G) = \{\pm I_{2n}\} \times \mathrm{Sp}_{2n-2}(q)$ where I_{2n} is $2n \times 2n$ identity matrix. In the case of $\mathrm{PSp}_{2n}(q)$, we have central product $C_G(i) = \mathrm{SL}_2(q) \circ \mathrm{Sp}_{2n-2}(q)$. By the same argument the image ζ_0^i does not contain involutions which do not lie in the center of $\mathrm{SL}_2(q)$ component since $n \geqslant 3$.

(b) Note that $C = C_G(i)$ is direct product of two copies of $\mathrm{SL}_2(q)$. Hence $I(C)$ is an elementary abelian group of order 4. By Lemma 3.3, ζ_0^i does not produce the involution i and iz where z is the central involution in $\mathrm{Sp}_4(q)$. Hence the image of ζ_0 contains only the central involution z and the result follows.

(c) If $G = \mathrm{PSp}_4(q)$, then $C_G(i) = (\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)) \rtimes \langle t \rangle$ where t is an involution interchanging the components. Again as ζ_0^i does not produce the involution i, it produces a pseudo-involution in both components of $C_G(i)$ or the involution t. In either case as $\heartsuit_i(G)$ is normal subgroup in $C_G(i)$, we conclude that $\heartsuit_i(G) \geqslant E(C_G(i)) = \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$. □

Glauberman Z^*-Theorem. [5, page 262] *Let G be a finite group and $i \in G$ be an involution such that $\{i^G\} \cap C_G(i) = \{i\}$. Then $i^* \in Z(G^*)$ where $G^* = G/O_{2'}(G)$ and $O_{2'}(G)$ is the maximal normal subgroup of odd order in G.*

We need the following consequence of Glauberman Z^*-Theorem to prove the next Theorem.

Lemma 3.8. *Let G be a non-abelian finite simple group and i be an involution in G. Then there exists an involution $j \in C_G(i)$ such that $j \neq i$ and $j^g = i$ for some $g \in G$.*

Theorem 3.9. *Let G be a finite simple group of Lie type over a field of odd characteristic p and $i \in G$ be an involution.*

- *If G is classical then $\heartsuit_i(G)$ contains the semisimple socle of $C_G(i)$ except for the groups $\mathrm{PSp}_{2n}(q)$ and involution of type t_1.*
- *If G is exceptional then $\heartsuit_i(G)$ contains at least one component in $C_G(i)$.*

Proof. Let i be an involution in G. We shall prove the claim by finding an involution in the image of ζ_0^i which does not centralize the component(s) in $C_G(i)$. If we find such an involution, then we will conclude that $\heartsuit_i(G)$ contains that component(s) of the semisimple socle of $C_G(i)$ since $\heartsuit_i(G)$ is a normal subgroup of $C_G(i)$. We will refer to Table 2.5 for the involution types and more information can be found in [25].

Let $G = \mathrm{PSL}_{n+1}(q)$, $n \geqslant 2$. If i is an involution of type t_1, then $C_G(i) \cong T \circ_{(n,q-1)} \mathrm{SL}_n(q)$ where T is a cyclic group of order $q-1$ and i is the only involution in $Z(C_G(i))$. Therefore there exists $g \in G$ such that $i^g \in C_G(i)$ by Lemma 3.8 which implies that $\zeta_0^i(g) = ii^g$ is not central in $C_G(i)$. Now assume that i is an involution of type t_k, $2 \leqslant k \leqslant n/2$, then the semisimple socle of $C_G(i)$ is $H = \mathrm{SL}_k(q) \circ \mathrm{SL}_{n+1-k}(q)$. Notice that there is an involution $s = s_1 s_2 \in H$ such that s_1 acts like an involution of type t_1 in $\mathrm{SL}_k(q)$ and s_2 acts like an involution of type t_{k-1} in $\mathrm{SL}_{n+1-k}(q)$. Hence the involution $s = s_1 s_2 \in H$ is an involution of type t_k in G and $s = i^g$ for some $g \in G$. Observe that $\zeta_0^i(g) = ii^g$ does not centralize neither of the components of H and hence $H \leqslant \heartsuit_i(G)$. Let $n+1$ be even and i be an involution of type $t'_{(n+1)/2}$, then $C_G(i)$ contains a subgroup $\frac{1}{((n+1)/2,q-1)}\mathrm{SL}_{(n-1)/2}(q^2)$ and i is the only involution in $Z(C_G(i))$. By Lemma 3.8, there is an element $g \in G$ such that $i^g \in C_G(i)$ and $\zeta_0^i(g) = ii^g$ is not central in $C_G(i)$. Therefore $\frac{1}{((n+1)/2,q-1)}\mathrm{SL}_{(n-1)/2}(q^2) \leqslant \heartsuit_i(G)$. The proof for $\mathrm{PSU}_n(q)$ is analogous.

Let $G = \Omega_{2n+1}(q)$ and $n \geqslant 3$. The proof for $n = 2$, we refer Lemma 3.7 (c) as $\Omega_5(q) \cong \mathrm{PSp}_4(q)$. Let V be the natural module for G. Then the dimension of the eigenspaces of the involutions of t_k or t'_k, $1 \leqslant k \leqslant n$, for the eigenvalue -1 is $2k$ and we denote these involutions by t_k to simplify the notation. Note that involution of type t_k or t'_k present in G if and only if $q^k \equiv 1 \bmod 4$ or $q^k \equiv -1 \bmod 4$ respectively. Let i be an involution of type t_1, then the semisimple socle of $C_G(i)$ is $H = \Omega_{2n-1}(q)$. Notice that there is a non-central involution s of type t_1 in H which is conjugate to i in G, say $s = i^g$ for some $g \in G$. Hence $H \leqslant \heartsuit_G(i)$ by similar arguments above. Assume now that i is an involution of type t_k, $2 \leqslant k < n$. We know that $C_G(i)$ contains a subgroup $H = \Omega_{2k}^{\varepsilon}(q) \times \Omega_{2(n-k)+1}(q)$ where $q^k \equiv \varepsilon \bmod 4$. Note that $\Omega_{2k}^{\varepsilon}(q)$ contains an involution s_1 which is conjugate to an involution of type t_{k-1} in G and

$\Omega_{2(n-k)+1}(q)$ contains an involution s_2 which is conjugate to an involution of type t_1 in G. It is clear that the involution $s = s_1s_2$ is conjugate to an involution of type t_k in G, hence $s = i^g$ for some $g \in G$. Since s_1 and s_2 are non-central involutions in the corresponding subgroups, $\zeta_0^i(g) = ii^g$ does not centralize neither of the components of H hence the result follows. If $i \in G$ is an involution of type t_n, then following the notation of Lemma 3.7, we have $\dim V_- = 2n$. The semisimple socle of $C_G(i)$ is $H = \Omega_{2n}^{\varepsilon}(q)$ where $q^n \equiv \varepsilon \bmod 4$. Observe that $ii^g \in C = C_{\mathrm{SL}(V)}(V_- \cap V_-g)$ for any $g \in G$. Since $\dim V_- = 2n$, $V_- \cap V_-g$ has codimension $\leqslant 2$ and $C/O_p(C)$ is a subgroup of $\mathrm{SL}_2(q)$. Notice also that we can choose $g \in G$ so that $i^g \in C_G(i)$ by Lemma 3.8. Hence $\zeta_0^i(g) = ii^g$ and it is clear that $\zeta_0^i(g)$ does not centralize H.

Let $G = \mathrm{PSp}_{2n}(q)$ and $n \geqslant 3$. We refer Lemma 3.7 (c) for the case $n = 2$ and for the involution of type t_1 we refer Lemma 3.7 (a). Let $i \in G$ be an involution of type t_k, $2 \leqslant k \leqslant n/2$, then $C_G(i)$ contains a subgroup $H = \mathrm{Sp}_{2k}(q) \circ_2 \mathrm{Sp}_{2n-2k}(q)$. Observe that $\mathrm{Sp}_{2k}(q)$ contains an involution s_1 which is conjugate to an involution of type t_{k-1} in G and $\mathrm{Sp}_{2n-2k}(q)$ contains an involution s_2 which is conjugate to an involution of type t_1 in G. As s_1 commutes with s_2, the involution $s = s_1s_2$ is conjugate to an involution of type t_k in G, hence $s = i^g$ for some $g \in G$. Since s_1 and s_2 are non-central involutions in the corresponding subgroups, $\zeta_0^i(g) = ii^g$ does not centralize neither of the components in the centralizer hence the result follows. If i is an involution of type t_n, then $C_G(i)$ contains a subgroup $\frac{1}{(2,n)}\mathrm{GL}_n^{\varepsilon}(q)$ where $q \equiv \varepsilon \bmod 4$. In either case we can apply Lemma 3.8 and find $g \in G$ such that $i^g \in C_G(i)$ and i^g is non-central in $C_G(i)$ as i is the only involution in $Z(C_G(i))$.

Let $G = \mathrm{P}\Omega_{2n}^{\varepsilon}(q)$ and $n \geqslant 4$. For the involutions of types t_k or t'_k, $1 \leqslant k < n-1$, the proof is similar to the case $G = \Omega_{2n+1}(q)$. If i is of type t_{n-1} or t_n, then $C_G(i)$ contains a subgroup $\frac{1}{2}\mathrm{GL}_n^{\varepsilon}(q)$ where $q \equiv \varepsilon \bmod 4$. In either case by Lemma 3.8, there exists $g \in G$ such that $i^g \in C_G(i)$ and i^g is non-central in $C_G(i)$ as $Z(C_G(i)) = \langle i \rangle$.

Let $G = {}^3D_4(q)$ or $G_2(q)$. Then there is only one conjugacy class of involutions in G. Let i be an involution in G, then $C_G(i) = \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q^3)$ or $\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$ respectively. Notice that there is an involution s in $C_G(i)$ which does not centralize either components and it is necessarily conjugate to i since there is only one conjugacy class of involutions. Let $s = i^g$ for some $g \in G$, then $\zeta_0^i(g) = ii^g$ does not centralize the components of the $C_G(i)$ and the result follows. We apply the same argument to the group ${}^2G_2(q)$ as there is only one conjugacy class of involutions in ${}^2G_2(q)$.

Let G be a group of type $F_4(q)$. Let i be an involution of type t_4, then $C_G(i)'' = \mathrm{Spin}_9(q)$ and $Z(C_G(i)) = \langle i \rangle$. By Lemma 3.8, there exists $g \in G$ such that $i \neq i^g \in C_G(i)$ and $\zeta_0^i(g) = ii^g$ is non-central in $\mathrm{Spin}_9(q)$. If i is an involution of type t_1, then $C_G(i) \cong \mathrm{SL}_2(q) \circ_2 \mathrm{Sp}_6(q)$ and $Z(C_G(i)) = \langle i \rangle$. Again, by Lemma 3.8, there exists $g \in G$ such that $\zeta_0^i(g) = ii^g$ is non-central in $\mathrm{Sp}_6(q)$. Hence $\mathrm{Sp}_6(q) \leqslant \heartsuit_i(G)$. By the same argument, if $\mathrm{SL}_2(q)$ is a component in the semisimple socle of $C_G(i)$ for $G = E_6(q)$, $E_7(q)$, $E_8(q)$, then $\heartsuit_i(G)$ contains the other quasi-simple component of semisimple socle of $C_G(i)$.

In the remaining exceptional groups $E_6^\varepsilon(q)$, $E_7(q)$ and $E_8(q)$, semisimple socles of the centralizers of involutions contain a single quasi-simple group if $\mathrm{SL}_2(q)$ does not appear, see Table 2.5, and the involution i is the only central involution in $C_G(i)$. Hence we apply previous arguments to these cases. □

Corollary 3.10. *Let G be a quasi-simple group of Lie type defined over a field of odd characteristic and $i \in G$ be a non-central involution in G.*

1. *If G is classical then $\heartsuit_i(G)$ contains the semisimple socle of $C_G(i)$ except for the groups $(\mathrm{P})\mathrm{Sp}_{2n}(q)$ and involution of type t_1.*

2. *If G is exceptional then $\heartsuit_i(G)$ contains at least one component in $C_G(i)$.*

Proof. Note that the non-central involutions in G map to involutions in $G/Z(G)$ and we apply the same arguments as in Theorem 3.9. □

In Theorem 3.9 and Corollary 3.10, it may happen that if $\mathrm{SL}_2(q)$ appears as a component in the centralizers of involutions in exceptional groups, then $\heartsuit_i(G)$ contains only the other component of $C_G(i)$. However the experiments in GAP showed that the semisimple socles of $C_G(i)$ is also included in $\heartsuit_i(G)$ in the exceptional groups G of Lie type.

Chapter 4

Construction of a long root $\mathrm{SL}_2(q)$-subgroup

Our aim in this chapter is to prove Theorem 1.1. We achieve this in two steps. First, we present an algorithm that constructs a long root $\mathrm{SL}_2(q)$-subgroup in a finite simple group G of Lie type defined over the field of odd order q. Then in Section 4.2 we extend this algorithm for groups with non-trivial p-core.

4.1 Constructing a long root $\mathrm{SL}_2(q)$-subgroup in simple groups

Let G be a group and $G_i \leqslant G$, $i = 1, \ldots, n$. Assume that

$$G = \langle G_i \mid i = 1, \ldots n \rangle$$

and G_k commutes with G_l for any $k \neq l$. Then we say that G is *commuting products* of G_i for $i = 1, \ldots, n$.

Algorithm 4.1. "Construction of a long root $\mathrm{SL}_2(q)$-subgroup in a finite simple group of Lie type"

Input: A black box group isomorphic to a finite simple group G of Lie type defined over a field of odd size q except $\mathrm{PSL}_2(q)$ and ${}^2G_2(q)$.

Output: A black box group which is a long root $\mathrm{SL}_2(q)$-subgroup in G.

Description of the algorithm:
Step1: Construct the centralizers of involutions recursively to find a commuting products of $(\mathrm{P})\mathrm{SL}_2(q^k)$ in G where $k \geqslant 1$ may vary, Algorithm 4.2.
Step 2: Construct one of the components $(\mathrm{P})\mathrm{SL}_2(q^k)$ in the commuting product and check whether it is a long root $\mathrm{SL}_2(q)$-subgroup of G, Algorithm 4.12 and 4.14.

Note that in Step 1, we may have commuting products of $(\mathrm{P})\mathrm{SL}_2(q)$ where q may vary but the characteristic of the underlying field is fixed, for example, in $G = {}^3D_4(q)$ there is only one conjugacy class of involutions and $C_G(i) \cong \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q^3)$ for an involution $i \in G$.

4.1.1 Constructing commuting products of $(\mathrm{P})\mathrm{SL}_2(q)$

We first construct commuting products of $(\mathrm{P})\mathrm{SL}_2(q)$ in G by recursive construction of the centralizers of involutions using the function $\zeta^i = \zeta_0^i \sqcup \zeta_1^i$.

Algorithm 4.2. "Construction of a commuting products of $(\mathrm{P})\mathrm{SL}_2(q)$-subgroup"

Input: A black box group isomorphic to a finite simple group G of Lie type defined over a field of odd size q except $\mathrm{PSL}_2(q)$ and ${}^2G_2(q)$.

Output: A black box group which is commuting products of $(\mathrm{P})\mathrm{SL}_2(q^k)$ for various $k \geqslant 1$.

Description of the algorithm:
Step 1: Produce an involution $i = \mathrm{i}(g)$ from a random element $g \in G$ and check whether it is central or not. If it is always central after several attempts then return G.
Step 2: Produce sufficiently many elements $S = \{g_1, \ldots, g_s\} \subset G$ and construct $\zeta^i(S) \leqslant C_G(i)$.
Step 3: Construct $\zeta^i(S)''$, second derived subgroup of $\zeta^i(S)$.

1. If $\zeta^i(S)'' \neq 1$ then set $G = \zeta^i(S)''$ and go to Step 1.
2. If $\zeta^i(S)'' = 1$, then construct $H = \langle i^G \rangle$.
   - If ζ_1^i is used in the generation of $\zeta^i(S)$, then we return H.
   - If ζ_1^i is not used in the generation of $\zeta^i(S)$ then we look for a pseudo-involution $j \in H$ and check whether
   $$\zeta^j(T)'' \neq 1$$
   for a subset $T \subset H$. If $\zeta^j(T)'' = 1$ then we return H. If $\heartsuit_j(H)'' \neq 1$ then H is products of $\mathrm{Sp}_4(q)$ and we use ζ_1^i map to construct $C_H(i)$ which is in turn isomorphic to direct products of $\mathrm{SL}_2(q)$ and

return $C_H(i)$. Here i is the involution produced in Step 1. Note that this part deals with the exception in Theorem 3.9, that is, $\heartsuit_i(G)'' = 1$ where $G = \mathrm{Sp}_4(q)$ and $i \in G$ is an involution of type t_1.

The involution $i = \mathrm{i}(g)$ for a random element g

We pick a random element $g \in G$ and produce the involution $i = \mathrm{i}(g)$. To produce an involution from a random element, we need an element of even order. The share of these elements is given by the following theorem.

Fact 4.3. ([31]) *Let G be a finite group having a simple homomorphic image that is neither cyclic nor Lie type of characteristic 2. Then the share of elements having an even order is at least $1/4$.*

Next, we need to check whether $i = \mathrm{i}(g)$ is central in G or not. Notice that this procedure is unavoidable in the recursive steps of our algorithm as $C_G(i)''$ contains central involutions in most of the cases (see Table 2.5). As a set of generators of G is a part of input we can check whether i commutes with the generators of G. We can find a non-central involution in view of the following lemma.

Lemma 4.4. *Let G be a universal version of a finite group of Lie type defined over a field of odd characteristic. Then the share of elements in G producing non-central involutions is bounded from below by a function of the Lie rank of G.*

Proof. Let T be any maximal torus corresponding to an element w in the Weyl group W as in Section 2.5. Then $|N_G(T)/T| = |C_W(w)|$ by Theorem 2.16. Therefore the number of tori conjugate to T in G is at least

$$\frac{|G|}{|T||C_W(w)|}.$$

Hence the probability of being an element in a torus conjugate to T is at least

$$\frac{1}{|C_W(w)|}.$$

Therefore if T is any torus containing an involution i then the number of elements producing i depends only on W not on the size of the field. In classical

groups, tori twisted by the cycles of length less than the length of the longest cycle do not contain central involutions. This observation immediately follows from the tables of the centralizers of involutions and the orders of the corresponding tori, see Section 2.5. Note that among the exceptional groups only $E_7(q)$ has central extension which has central involution in which case one can use the same argument to get the conclusion. □

We give an example in the easiest case. Let $G = \mathrm{SL}_n(q)$, n even and $n \geqslant 5$. Then a maximal torus T twisted by a product of $n-2$ and 2 cycles is of the form $T = T_1 \circ_{q-1} T_2$ where T_1 is a cyclic group of order $(q^{n-2}-1)$ and T_2 is a cyclic group of order (q^2-1), see [18] and Section 2.5. Note that as n is an even number (q^2-1) divides $(q^{n-2}-1)$ and therefore involutions produced from random elements in T belongs to T_1 with probability very close to 1. It can be observed from Table 2.5 that T_1 has involution i of type t_2 in G by comparing the orders of $C_G(i)$ and T_1. Since $W = \mathrm{Sym}(n)$, symmetric group on n letters, and $n \geqslant 5$, $C_W(w)$ has order $2(n-2)$. Therefore the probability of producing non-central involutions in G from random elements is at least $\frac{1}{2(n-2)}$.

Hence after feasible number of iterations we will find a non-central involution $i = \mathrm{i}(g)$ in G by Lemma 4.4. If we are always in a situation of producing central involutions then we use a result by Griess [26] to conclude that G is isomorphic to direct products of $\mathrm{SL}_2(q)$. In this case, we take this subgroup as an output.

Recursion

Let $i = \mathrm{i}(g)$ be a non-central involution in G. Then we construct $\zeta^i(S)$ for a subset $S \subset G$. If ζ_1^i is defined for good sample of elements in S, then $\zeta^i(S) = C_G(i)$ with probability close to 1, especially over large fields, by Fact 3.1 together with the following theorem.

Fact 4.5. ([33, 38]) *Two randomly chosen elements in a finite simple group G generates G with probability which tends to 1 as $|G|$ tends to ∞.*

If ζ_1^i is not defined for S, then ζ_0^i is defined for all the elements in S and we use only the function ζ_0^i. Recall that the image of the map ζ_0^i in G is a normal subset of $C_G(i)$ by Fact 3.1 but ζ_0^i does not produce uniformly distributed random elements in $C_G(i)$. In this case we take S to be sufficiently large so that we have $\zeta_0^i(S) = \heartsuit_i(G)$. It turns out that $\zeta_0^i(S) = \heartsuit_i(G)$ for a reasonably sized subset $S \subset G$ regarding our experiments in GAP. A reasonable number

of generators for $\heartsuit_i(G)$ produced by ζ_0^i is, for example, 50 for 50×50 matrix groups. We note here two results of Liebeck and Shalev.

Fact 4.6. ([39]) *Let G be a finite simple group and $S \subseteq G$ a normal subset. Then there exists a constant c such that $S^n = G$ for any $n \geqslant c\log|G|/\log|S|$.*

Fact 4.7. ([39]) *There exists a constant c such that for any element of any finite simple group G can be written as a product of c involutions.*

If the algorithm fails to succeed in constructing of a commuting products of (P)$\mathrm{SL}_2(q)$ for various q, for example, it may return the identity group, it might happen that we fail to construct the component(s) of the centralizers of involutions in the recursive steps in which case we use the same involutions to produce more generators for the centralizers of involutions constructed previously in the recursive steps.

From now on we assume that S is sufficiently large so that we have $\heartsuit_i(G) \leqslant \zeta^i(S)$, and by definition $\zeta^i(S) \leqslant C_G(i)$.

The derived subgroup

We will construct the semisimple socle of $\zeta^i(S)$ for the involution $i \in G$. By Lemma 2.18, $\zeta^i(S)''$ is the semisimple socle of $\zeta^i(S)$. If $\zeta^i(S) = \heartsuit_i(G)$, then $\zeta^i(S)''$ contains at least one component of the semisimple socle of $C_G(i)$ by Lemma 2.18 and Theorem 3.9.

Assume that we are at the k^{th} recursive step of our algorithm, namely

$$C_{i_k} = \zeta^{i_k}(S_k)''$$

where $i_k = \mathrm{i}(g)$, $g \in C''_{i_{k-1}}$ and $S_k \subset C''_{i_{k-1}}$. Set $H = C''_{i_{k-1}}$.

If $C''_{i_k} = 1$, then either

- $\langle i_k^H \rangle$ is a commuting products of (P)$\mathrm{SL}_2(q)$ by Lemma 3.4 and 3.5; or
- $\langle i_k^H \rangle$ is a commuting products of $\mathrm{Sp}_4(q)$ which is the case if $C_{i_k} = \heartsuit_{i_k}(H)$, and i_k is of type t_1 in the correponding components, see Lemma 3.4 and Lemma 3.7(b).

If $C''_{i_k} \neq 1$, then we set $G = C''_{i_k}$ and go to Step 1.

Assume that $C''_{i_k} = 1$. If the map $\zeta_1^{i_k}$ is used in the generation of $\zeta^{i_k}(S_k)$, then we assume that $C_{i_k} = C_H(i_k)$ by Facts 3.1 and 4.5. Hence the subgroup $\langle i_k^H \rangle'$ is a commuting products of (P)$\mathrm{SL}_2(q)$ and we return this subgroup.

If $\zeta_1^{i_k}$ is not used in the generation of $\zeta^{i_k}(S_k)$, then H may be direct products of $\mathrm{Sp}_4(q)$ and i_k is an involution of type t_1. To distinguish commuting products of (P)$\mathrm{SL}_2(q)$ from direct products of $\mathrm{Sp}_4(q)$, we look for a pseudo-involution $j \in H$.

Let H be a commuting products of several (P)$\mathrm{SL}_2(q)$. If we can not find any pseudo-involution in H, then we deduce that H is a direct products of $\mathrm{PSL}_2(q)$ and we go to Step 1 and start the procedure from the very beginning since long root $\mathrm{SL}_2(q)$-subgroups are isomorphic to $\mathrm{SL}_2(q)$ by Theorem 2.14. Now let $j \in H$ be a pseudo-involution and

$$Y = \langle j^H \rangle'.$$

Then $C_Y(j)'' = 1$ and hence $\zeta^j(T)'' = 1$ for any subset $T \subset Y$. On the other hand, if H is direct products of $\mathrm{Sp}_4(q)$, then by Theorem 3.9, Lemmas 2.18 and 3.4, $\zeta^j(T)''$ is direct products of $\mathrm{SL}_2(q)$, we used here the assumption that $\heartsuit_j(Y) \leqslant \zeta^j(T)$.

Summarizing this observation if we have $\zeta^j(T)'' = 1$ then Y is a commuting products of $\mathrm{SL}_2(q)$ and we take Y as an output. If $\zeta^j(T)'' \neq 1$ then we have commuting products of $\mathrm{Sp}_4(q)$ and i_k acts as an involution of type t_1 in the corresponding components so we use the function $\zeta_1^{i_k}$ to construct $C_H(i_k)$ which is isomorphic to direct products of $\mathrm{SL}_2(q)$. For the share of elements in $\mathrm{Sp}_4(q)$ defining the map $\zeta_1^{i_k}$ see Theorem 5.11.

Note that if $G = \mathrm{Sp}_4(q)$ and j is a pseudo-involution, then $C_G(j)''$ is a short root $\mathrm{SL}_2(q)$-subgroup in G [32].

We apply the following theorem in construction of the derived subgroup of a black box group.

Fact 4.8. ([8]) *The commutator subgroup of a black box group can be constructed in Monte–Carlo polynomial time.*

4.1.2 Finding $\mathrm{SL}_2(q)$

The aim of this section is to construct a normal subgroup $\mathrm{SL}_2(q^k)$ which appears as a factor in a given commuting products of (P)$\mathrm{SL}_2(q^l)$ for various l found in Section §4.1.1.

Let $K = \mathrm{SL}_2(q)$. It is well known that all semisimple elements in $K \backslash Z(K)$ are regular, therefore they belong to only one torus. There are two conjugacy classes of tori in K, split and non-split tori. The split torus is a cyclic group of order $q-1$ and the non-split torus is a cyclic group of order $q+1$.

Lemma 4.9. *Let $K = \mathrm{SL}_2(q)$, $q > 3$, and $L = K \times K$. Then the probability of producing a pseudo-involution acting non-trivially on only one component is at least* $1/24$.

Proof. Let T_1 be a split torus in G, then

$$|K : N_K(T_1)| = q(q+1)/2.$$

Let T_2 be a non-split torus in G, then

$$|K : N_K(T_2)| = q(q-1)/2.$$

Hence total number of tori is q^2. Therefore the probability of a semisimple element belonging to a split torus is

$$\frac{1}{2}\frac{q(q+1)}{q^2} > \frac{1}{2}$$

and to a non-split torus is

$$\frac{1}{2}\frac{q(q-1)}{q^2} \approx \frac{1}{2} > \frac{1}{3}$$

since $q > 3$. Let $g = (g_1, g_2) \in L$. Then g_1^q and g_2^q belong to different classes of tori in L with probability at least $1/6$. Note that one of the tori has order divisible by 4 and in this torus the probability of finding an element whose order is divisible by 4 is at least $1/4$. Therefore a pseudo-involution produced from a random element acts non-trivially on only one component in L with probability at least $1/24$. □

We can state an immediate corollary:

Corollary 4.10. *Let L be a commuting products of $\mathrm{SL}_2(q)$. Then we can find a pseudo-involution which acts non-trivially in fewer number of components in L with probability at least* $1/24$.

Lemma 4.11. *Let $K = \mathrm{SL}_2(q)$ and $t \in K$ be a pseudo-involution. Then elements of the form tt^g have odd order with probability at least* $1/6$.

Proof. It follows from the above observation that the semisimple elements of the form $z = tt^g$, $g \in K$, belongs to a torus of order $q-1$ or $q+1$. The probability that z belongs to a certain type of torus is at least $1/3$ by the proof of Lemma 4.9 and one of $(q \pm 1)/2$ is an odd number. Therefore z has odd order with probability at least $1/6$. □

Algorithm 4.12. "Construction of $\mathrm{SL}_2(q)$"

Input: A black box group L which is isomorphic to commuting products of $(\mathrm{P})\mathrm{SL}_2(q^l)$ for various l.

Output: A black box group isomorphic to $\mathrm{SL}_2(q^k)$ for some k appearing as a factor in the commuting product or return the statement "L is direct products of $\mathrm{PSL}_2(q^l)$ for various l".

Description of the algorithm:
Step1: Produce a pseudo-involution $t \in L$. If we can not find any pseudo-involution then return "L is direct products of $\mathrm{PSL}_2(q^l)$ for various l".

Recall that the elements of $\mathrm{SL}_2(q)$ belong to a cyclic subgroup of order $q \pm 1$ and one of the numbers $(q \pm 1)/2$ has even order and at least half of the elements in the corresponding cyclic subgroup are also of even order. Therefore we can find elements whose orders are multiple of 4 with probability at least 1/4. Hence we can produce a pseudo-involution from random elements by following the procedure in Section 3.1. If we can not find a pseudo-involution in L, then we deduce that L is a direct products of $\mathrm{PSL}_2(q)$ and we start the procedure from the very beginning, that is, we go back to Algorithm 4.2.

Step2: Construct $\zeta_1^t(S)''$ for some $S \subset L$. If the map ζ_1^t does not work, then construct $\langle t^L \rangle'$.

Note that we may be in a situation of not to be able to use the map ζ_1^t for some subset $S \subset L$ when t acts as a pseudo-involution in a big number of components, see Remark 3.2. If we fail to use the map ζ_1^t then we construct $K = \langle t^L \rangle'$ and set $L = K$ and go to Step1. However if the map ζ_1^t works, then t is a pseudo-involution in a small number of components and we construct $\zeta_1^t(S)$, see Lemma 4.11. We can assume that $\zeta_1^t(S) = C_L(t)$ by Facts 3.1 and 4.5. Let $C = \zeta_1^t(S)''$, then C does not contain the components where t acts as a pseudo-involution in the commuting product by Lemma 3.6. Therefore we have smaller number of components in the subgroup C and if $C \neq 1$, then we set $L = C$ and go to Step 1. We can check whether $C \neq 1$ by producing a random element in C and comparing it with 1. If $C = 1$, then we return to Step 1. Observe that if we always have $C = 1$ in m times, then we deduce that $L = \mathrm{SL}_2(q^k)$ for some k in the commuting product where the probability of error is at most $(1 - 1/24)^m$, see Corollary 4.10.

4.1.3 Finding the order of the field

In this section, we find the order of the field in the subgroup $(\mathrm{P})\mathrm{SL}_2(q)$ constructed in the previuos section.

Algorithm 4.13. "Finding field order"

Input: A black box group K isomorphic to $(\mathrm{P})\mathrm{SL}_2(q)$.

Output: The order q of the underlying field.

Description of the algorithm:

The elements of K have order dividing either $q-1$ or $q+1$ or $2p$. Here p is the characteristic of the field. The semisimple elements belong to tori of order $q \pm 1$. The probability of finding a generator in these tori is

$$\frac{\Phi(q \pm 1)}{q \pm 1} \geqslant \frac{1}{e^{\gamma} \log\log(q \pm 1)}$$

where Φ is Euler function, e is the base of the natural logarithm and γ is Euler constant [41]. Therefore we can find an element of order $q \pm 1$ with probability at least $1/e^{\gamma} \log\log(q \pm 1)$.

Let $E = p^n m$, $(p, m) = 1$, be a global exponent for the group G which is the input group in Algorithm 4.1. We produce sufficiently many elements $g_1, \ldots, g_s \in K$. It is clear that $g_l^{p(p^n-1)} = 1$ for each $l = 1, \ldots, s$. Starting from $k = 1$, we check whether $g_i^{p(p^{2k}-1)} = 1$ for each $l = 1, \ldots, s$. When we find the smallest such number k, $1 \leqslant k \leqslant n$, we deduce that the order of the undelying field is $q = p^k$. The probability of error is at most $(1 - 1/e^{\gamma} \log\log(q \pm 1))^s$.

Note that the order of the field found by Algorithm 4.13 is not necessarily the order of the field on which G is defined, for example, let $G = \mathrm{PSL}_4(q)$ and $q \equiv -1 \bmod 4$, then there exists an involution $i \in G$ such that $K = C_G(i)'' = \mathrm{PSL}_2(q^2)$ and Algorithm 4.13 returns q^2. In this case, observe that K is not a subsystem subgroup in G.

4.1.4 A long root $\mathrm{SL}_2(q)$

The aim of this section is to prove Theorem 1.2, that is, we present an algorithm which decides the subgroup K found in Section 4.1.2 is a long root

$\mathrm{SL}_2(q)$-subgroup in a finite simple group G of Lie type of odd characteristic. Here q is the order of the field found in Section 4.1.3 for K.

Algorithm 4.14. "Checking whether a given (P)$\mathrm{SL}_2(q)$ is a long root $\mathrm{SL}_2(q)$"

Input: A black box group K which is known to be isomorphic to (P)$\mathrm{SL}_2(q)$ *for some q in G.*

Output: The truth value of the statement: "K is a long root $\mathrm{SL}_2(q)$*-subgroup in G".*

Description of the algorithm:
Step 1: Produce an involution $z \in K$ and check whether it is central in K or not. If $z \in Z(K)$, then go to next step, otherwise return the statement 'K is not long root $\mathrm{SL}_2(q)$-subgroup'.

If $z \notin Z(K)$, then $K = \mathrm{PSL}_2(q)$ and we deduce that K is not a long root $\mathrm{SL}_2(q)$-subgroup by Theorem 2.14.

Step 2: Construct $C = \zeta^z(S)''$ for some subset $S \subset G$.
Step 3: Construct $N = \langle K, K^g \rangle$ for $g \in C$. If we find an element $n \in N$ satisfying $n^{q(q^2-1)} \neq 1$, then we conclude that K is not a long root $\mathrm{SL}_2(q)$-subgroup. If we can not find such an element after reasonable number of times, then we repeat this step for another $g \in C$. If we always have $n^{q(q^2-1)} = 1$, then we conclude that K is a long root $\mathrm{SL}_2(q)$-subgroup.

We may assume that $K = \mathrm{SL}_2(q)$ where q is found by Algorithm 4.13 for K. We know that if K is a long root $\mathrm{SL}_2(q)$-subgroup in G, then $K = K^g$ for any $g \in C$ by Corollary 2.20.

If K is not a long root $\mathrm{SL}_2(q)$-subgroup, then we shall prove that K is contained strictly in the subgroup $N = \langle K, K^g \rangle$ for a random $g \in C$ with probability close to 1 except for the groups $G_2(q)$ and ${}^3D_4(q)$. Therefore $K \neq N$, and as soon as we find an element in N whose order does not divide $q(q^2-1)$, we deduce that K is not a long root $\mathrm{SL}_2(q)$-subgroup in G. Note that if K is not a long root $\mathrm{SL}_2(q)$-subgroup then either K is a short root $\mathrm{SL}_2(q)$-subgroup or the order of the field is increased in the construction of K (see the example at the end of previous section).

Assume first that the order of the field is increased in the construction of K. This is possible only in $G = \mathrm{PSL}_n^{\varepsilon}(q)$ with n even, and $C_G(i)'' = \frac{1}{(n/2,q-1)}\mathrm{SL}_{n/2}(q^2)$, see Table 2.5. Assume that $G = \mathrm{PSL}_n(q)$ and we obtain $K = \mathrm{SL}_2(q^{2^k})$ for some $k \geqslant 1$ by constructing centralizers of involutions recursively. Note that K can be embedded naturally in $L = \mathrm{SL}_{2^{k+1}}(q)$ and $C_G(z)'' \cong \mathrm{SL}_{2^{k+1}}(q) \circ \mathrm{SL}_{n-2^{k+1}}(q)$. Now let $K_1 \cong \mathrm{SL}_2(q^{2^{k-1}})$ be a subgroup in K. Then $N_1 = \langle K_1, K_1^g \rangle = \mathrm{SL}_4(q^{2^{k-1}})$ with probability at least $1 - O(1/q^{2^{k-1}})$ for $g \in C_G(z)''$, see Lemma 5.6, and $N_1 \leqslant L$. Now $N_1 < N = \langle K, K^g \rangle$ and N_1 contains sufficiently many elements of order not dividing $q^{2^k}(q^{2^{k+1}} - 1)$. The case $G = \mathrm{PSU}_n(q)$ is analogous.

If K is a short root $\mathrm{SL}_2(q)$-subgroup, then, by Table 2.4, $K = \mathrm{PSL}_2(q^2)$, $\mathrm{PSL}_2(q)$ or $\mathrm{PSL}_2(q^2)$ for $G = \mathrm{PSU}_n(q)$, $\Omega_{2n+1}(q)$, $\mathrm{P}\Omega_{2n}^-(q)$ respectively. These cases are recognized in Step 1. Therefore we are left with the cases $G = \mathrm{PSp}_{2n}(q)$, $F_4(q)$ or ${}^2E_6(q)$.

Let $G = \mathrm{PSp}_{2n}(q)$, then $K \cong \mathrm{SL}_2(q)$. Let $z \in Z(K)$, then $C_G(z)'' = \mathrm{Sp}_4(q) \circ_2 \mathrm{Sp}_{2n-4}(q)$ and K is contained in $\mathrm{Sp}_4(q)$. We have $N = \langle K, K^g \rangle = \mathrm{Sp}_4(q)$ with probability close to 1 for random $g \in C_G(z)''$, which follows from a similar idea of the proof of Lemma 5.7, and N contains sufficiently many elements of order not dividing $q(q^2 - 1)$. If $G = F_4(q)$, then $K = \mathrm{SL}_2(q)$ and $C = C_G(z)'' = \mathrm{Spin}_9(q)$. Since $C/Z(C) \cong \Omega_9(q)$, it is enough to obtain the estimates in $G = \Omega_9(q)$. Let K be a short root $\mathrm{SL}_2(q)$-subgroup in G, then $K \cong \mathrm{PSL}_2(q)$ and $[K, V]$ is a orthogonal 3-space of Witt index 1 where V is the natural module for G. Now, following the same idea in the proof of Lemma 5.8, we obtain that $N/Z(N) \cong \mathrm{P}\Omega_6^+(q)$ with probability at least $1 - O(1/q)$ where $N = \langle K, K^g \rangle$ and $g \in G$. It is clear that N contains sufficiently many elements whose orders do not divide $q(q^2 - 1)$. If $G = {}^2E_6(q)$, then $K = \mathrm{SL}_2(q^2)$, $C = C_G(z)'' = \mathrm{Spin}_{10}^-(q)$ and $C/Z(C) \cong \mathrm{P}\Omega_{10}^-(q)$. In this case we find a similar estimate in $\Omega_{10}^-(q)$. Note that if K is a short root $\mathrm{SL}_2(q)$-subgroup in $\Omega_{10}^-(q)$, then $[K, V]$ is a orthogonal 4-space of Witt index 1 where V is the natural module for $\Omega_{10}^-(q)$. The rest is similar to the arguments above.

If we can not find an element $n \in N$ satisfying $n^{q(q^2-1)} \neq 1$, then we conclude that K is a long root $\mathrm{SL}_2(q)$-subgroup of G. Observe that this approach fails to recognize long root $\mathrm{SL}_2(q)$-subgoups in the

groups $G_2(q)$ and ${}^3D_4(q)$, see Lemma 2.21. We will deal with these exceptions in the next section. Notice that the output "K is not a long root $\mathrm{SL}_2(q)$-subgroup" is always true.

Remark 4.15. If Algorithm 4.14 returns a negative answer, then K is not a long root $\mathrm{SL}_2(q)$-subgroup, and instead of going back to the Algorithm 4.2 to construct new commuting products of $(\mathrm{P})\mathrm{SL}_2(q)$, we can construct another factor $(\mathrm{P})\mathrm{SL}_2(q)$ in L. Here L is a commuting products of $(\mathrm{P})\mathrm{SL}_2(q)$ constructed by Algorithm 4.2. To do this, we construct $M = C_L(z)''$ by using ζ_1^z, see Remark 3.2, where z is an involution or pseudoinvolution in K if $K = \mathrm{PSL}_2(q)$ or $\mathrm{SL}_2(q)$ respectively. If $M = 1$, then we go back to Algorithm 4.2 to construct new commuting products of $(\mathrm{P})\mathrm{SL}_2(q)$, see Lemmas 3.5 and 3.6. If $M \neq 1$, then it is commuting products of $(\mathrm{P})\mathrm{SL}_2(q)$ and we construct new component $K = (\mathrm{P})\mathrm{SL}_2(q)$ in M by using Algorithm 4.12 and find the order of the field in K by using Algorithm 4.13. Now we can run Algorithm 4.14 for this K.

The groups $G_2(q)$ and ${}^3D_4(q)$

In this section we present an algorithm which constructs a long root $\mathrm{SL}_2(q)$-subgroup in $G_2(q)$ and ${}^3D_4(q)$. We first present an algorithm which decides whether a given finite simple group of Lie type defined over a field of odd order is isomorphic to $G_2(q)$ or ${}^3D_4(q)$.

Algorithm 4.16. "$G_2(q)$ OR ${}^3D_4(q)$"

Input: A black box group isomorphic to a quasi-simple group of Lie type of odd characteristic.

Output: If G is isomorphic to $G_2(q)$ or ${}^3D_4(q)$, then it returns the statement 'It is isomorphic to $G_2(q)$ or ${}^3D_4(q)$ with probability close to 1'. Otherwise it returns 'It is not $G_2(q)$ or ${}^3D_4(q)$'.

DESCRIPTION OF THE ALGORITHM:
We present an algorithm for simple groups of Lie type; an idea of an algorithm for quasi-simple groups of Lie type is similar.

We check whether we get a commuting product of $\mathrm{SL}_2(q)$-subgroups from the first iteration of the recursive steps of Algorithm 4.2. If this is not the case, then we return 'It is not $G_2(q)$ or ${}^3D_4(q)$'. Otherwise we check whether Algorithms 4.12 and 4.14 returns a long root $\mathrm{SL}_2(q)$-subgroups. If

not, then we return 'It is not $G_2(q)$ or ${}^3D_4(q)$'. Otherwise we repeat the process from the begining and if we repeat this process more than a pre-set reasonable number of times we return 'It is isomorphic to $G_2(q)$ or ${}^3D_4(q)$ with probability close to 1'.

It follows directly from Table 2.5 that Algorithm 4.2 may return commuting product of $\mathrm{SL}_2(q)$-subgroups in the first iteration of the recursive steps in the following groups:

$$\mathrm{PSL}_3^\varepsilon(q), \mathrm{PSL}_4^\varepsilon(q), \mathrm{PSp}_4(q), \Omega_7(q), \mathrm{P}\Omega_8^\pm(q), G_2(q), {}^3D_4(q).$$

Let G be one the groups $\mathrm{PSL}_4^\varepsilon(q), \mathrm{PSp}_4(q), \Omega_7(q)$ or $\mathrm{P}\Omega_8^\pm(q)$. Then there is an involution $i \in G$ where $C_G(i)'' = \mathrm{PSL}_2(q^2), \mathrm{PSL}_2(q), \Omega_5(q)$ or $\Omega_6^\varepsilon(q)$ respectively, see Table 2.5. The probability of producing such an involution $i \in G$ is bounded from below by a universal constant since it depends only on the corresponding Weyl group, see Section 4.3 for similar computations. The subgroups $\mathrm{PSL}_2(q^2)$, $\mathrm{PSL}_2^\varepsilon(q)$ are not long root $\mathrm{SL}_2(q)$-subgroups in the corresponding groups which can be detected by Algorithm 4.14 and the subgroups $\Omega_5(q), \Omega_6^\varepsilon(q)$ are not commuting products of $(\mathrm{P})\mathrm{SL}_2(q)$ which can be detected by Algorithm 4.2. Hence we can assume now that $G = \mathrm{PSL}_3^\varepsilon(q), G_2(q)$ or ${}^3D_4(q)$, then $C_G(i)'' = \mathrm{SL}_2(q), \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$ or $\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q^3)$ respectively. It is clear that $\mathrm{SL}_2(q)$ has only central involutions whereas $\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$ and $\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q^3)$ have non-central involutions. Therefore $G_2(q)$ and ${}^3D_4(q)$ can be told apart by looking at the list above and hence among all finite simple groups of Lie type of odd characteristic. Observe that we do not use the size q of the field in the above arguments.

Algorithm 4.17. "Construction of a long root $\mathrm{SL}_2(q)$ in $G_2(q)$ and ${}^3D_4(q)$"

Input: A black box group G isomorphic to $G_2(q)$ or ${}^3D_4(q)$.

Output: A black box group K which is a long root $\mathrm{SL}_2(q)$-subgroup in G.

Description of the algorithm:
We construct a subgroup $K = \mathrm{SL}_2(q^k)$, for some k, by using Algorithm 4.1 where Algorithm 4.14 returns that K is a long root $\mathrm{SL}_2(q^k)$-subgroup in G. Note that if $G = {}^3D_4(q)$, then Algorithm 4.2 returns $\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q^3)$

and Algorithm 4.14 may return $K = \mathrm{SL}_2(q^3)$ and hence Algorithm 4.13 returns q^3. In this case $q^3 = p^k$ for some $k \geqslant 3$ and $q = p^{k/3}$. As the characteristic of the field is known, we find k and if it is not divisible by 3, then we conclude that the size of the field is correct. If $q = p^{3k_0}$, then we produce sufficiently many elements $g \in G$ and check whether $g^m = 1$ where $m = q_0^{12}(q_0^8 + q_0^4 + 1)(q_0^6 - 1)(q_0^2 - 1)$ and $q_0 = p^{k_0}$. Note that

$$|G_2(q)| = q^6(q^6 - 1)(q^2 - 1)$$

and

$$|{}^3D_4(q)| = q^{12}(q^8 + q^4 + 1)(q^6 - 1)(q^2 - 1).$$

If we find an element $g \in G$ such that $g^m \neq 1$, then we deduce that p^{3k_0} is the size of the underlying field and we use $q = p^{3k_0}$. After finding the size of the field, we can distinguish the groups ${}^3D_4(q)$ and $G_2(q)$. If $G = {}^3D_4(q)$, then we can find an element $g \in G$ such that $g^m \neq 1$ where $m = q^6(q^6-1)(q^2-1)$. However there are no such elements in $G_2(q)$. Therefore if we find such an element then we deduce that $G = {}^3D_4(q)$ otherwise $G = G_2(q)$.

Let $G = G_2(q)$ and $i \in G$ be an involution then $C_G(i) = L_1 \circ_2 L_2$ where $L_k \cong \mathrm{SL}_2(q)$, $k = 1, 2$. Notice that L_1 and L_2 are short and long root $\mathrm{SL}_2(q)$-subgroups in G. Assume that L_1 (resp. L_2) is short (resp. long) root $\mathrm{SL}_2(q)$-subgroup in G. Now let j be an involution in $C_G(i)$ which does not centralize L_1 and L_2. We have $C_G(j) = \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$ since there is only one conjugacy class of involutions in G. Let K_1 and K_2 be short and long root $\mathrm{SL}_2(q)$-subgroups in $C_G(j)$ respectively. Then it is easy to see that all the pairs $\{L_s, K_t\}$, $s, t = 1, 2$, generate $G_2(q)$ except $\langle L_2, K_2\rangle = \mathrm{SL}_3(q)$ or $\mathrm{SU}_3(q)$ [37]. Now we can distinguish $G_2(q)$ from $\mathrm{SL}_3^{\varepsilon}(q)$ by using Algorithm 4.16

Let $G = {}^3D_4(q)$ and $i \in G$ be an involution, then $C_G(i) \cong \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q^3)$ where $\mathrm{SL}_2(q)$ corresponds to long root and $\mathrm{SL}_2(q^3)$ corresponds to a short root $\mathrm{SL}_2(q)$-subgroups in G, see Table 2.4. To construct $\mathrm{SL}_2(q)$ we do the following. Let S be a set of generators for $C_G(i)$. Setting $m = q(q-1)(q+1)$, we consider

$$S^m = \{g^m \mid g \in S\}.$$

Now $L = \langle S^m\rangle = \mathrm{SL}_2(q^3)$ and we construct an element $g \in C_G(i)$ such that $g \in C_{C_G(i)}(L)$. Note that $(q-1, q^3+1) = (q+1, q^3-1) = 2$. Therefore we look for elements $g \in C_G(i)$ satisfying one of the conditions $g^{(q-1)(q^3+1)} = 1$

or $g^{(q+1)(q^3-1)} = 1$. Let $g = (g_1, g_2) \in C_G(i)$. Assume that $g^{(q-1)(q^3+1)} = 1$ where $g_1^{q-1} = 1$, $g_2^{q^3+1} = 1$ and g^{q^3+1} is non-central in $C_G(i)$. By repeating the proof of Lemma 4.9, we find such elements with probability at least 1/6 since the probability of finding a non-central element $g_1 \in \mathrm{SL}_2(q)$ of order dividing $q-1$ is at least 1/2 and the probability of finding an element $g_2 \in \mathrm{SL}_2(q^3)$ of order dividing q^3+1 is at least 1/3. Now, setting $h = g^{q^3+1}$ we have $\langle h^{C_G(i)} \rangle' = \mathrm{SL}(2,q)$ which is a long root $\mathrm{SL}(2,q)$-subgroup in G.

4.2 Groups with a non-trivial p-core

The aim of this section is to extend the algorithm for constructing long root $\mathrm{SL}_2(q)$-subgroups in the simple groups to the groups X where $X/O_p(X)$ is isomorphic to a finite simple group over a field of odd size $q > 3$, $q = p^k$ for some $k \geqslant 1$. Note that $O_p(X)$ is possibly trivial.

Algorithm 4.18. "Main Algorithm"

> *Input: A black box group X where $X/O_p(X)$ is isomorphic to a finite simple group over a field of odd size $q > 3$ and the characteristic p of the field.*
>
> *Output: A black box group K where $K/O_p(K)$ is a long root* $\mathrm{SL}_2(q)$*-subgroup in $X/O_p(X)$.*

The structure of the algorithm is same as in the previous algorithm.
Description of the algorithm:
Step1: Construct a subgroup L which is commuting products of subgroups K_s, $s \geqslant 1$, where $K_s/O_p(K_s)$ is isomorphic to (P)$\mathrm{SL}_2(q)$ for various q, by taking centralizers of involutions recursively.

> Let $i \in X$ be an involution and $C = C_X(i)$. By Corollary 2.19, $(C/O_p(C))''$ is the semisimple socle of $C/O_p(C)$. Therefore C'' is a central products of quasi-simple groups of Lie type of characteristic p extended by some p-group. Recall that the image of the function ζ_0^i consists of involutions, therefore if ζ_1^i is not used in some recursive steps in the generation of $C_X(i)$ then the resulting subgroup may have trivial p-core in which case we are in the situation of the previous setting and Algorithm 4.2 gives products of (P)$\mathrm{SL}_2(q)$ in X as desired. Therefore we assume that this does not happen. Note that it may happen that

the p-core is inverted by the involution i in which case ii^g are p-elements in $O_p(X)$ with probability close to 1 for random $g \in X$. In this case we construct the p-core and consider $C''/O_p(C'')$ and we use Algorithm 4.2. In all the other cases we obtain the products of subgroups K with the property that $K/O_p(K)$ is (P)$\mathrm{SL}_2(q)$.

Step2: Construct a subgroup K where $\bar{K} = K/O_p(K)$ is a long root $\mathrm{SL}_2(q)$ subgroup in $\bar{X} = X/O_p(X)$.

The construction of a subgroup K where $\bar{K}$ is (P)$\mathrm{SL}_2(q)$ follows from Algorithm 4.12. Now we shall check that $K/O_p(K)$ corresponds to a long root $\mathrm{SL}_2(q)$-subgroup in $X/O_p(X)$. Assume now that we have constructed K. We first produce an involution z in K, if $z \notin Z(K)$ and $C_K(z)'' = 1$, then we deduce that $K/O_p(K) \cong \mathrm{PSL}_2(q)$. Note that if $K/O_p(K) \cong \mathrm{PSL}_2(q)$ then $C_K(z)$ is a diheadral group of order $q \pm 1$ extended by a possibly non-trivial p-core, which has solubility degree 2. In this case we go to Step 1 and start the procedure from the beginning. Otherwise let $z \in Z(K)$, $C = C_X(z)$. We know that $C''/O_p(C'')$ is a product of quasi-simple groups by Lemma 2.19. If $\bar{K}$ is a long root $\mathrm{SL}_2(q)$-subgroup in $\bar{X}$, then, for any $x \in C''$, we have

$$K \leqslant \langle K, K^x \rangle \leqslant \langle K, K^y \rangle$$

for some $y \in O_p(K)$ (possibly trivial) which implies that $K = \langle K, K^x \rangle$. We have $g^{q(q^2-1)} = 1$ for any $g \in K$ whereas if $\bar{K}$ is not a long root $\mathrm{SL}_2(q)$-subgroup in $\bar{X}$, then we can find an element $x \in C''$ such that $K \neq \langle K, K^x \rangle$ and also we can find elements $g \in \langle K, K^x \rangle$ such that $g^{q(q^2-1)} \neq 1$ by using the same methods in Algorithm 4.14. If we find such an element the we return to Step 1 and start the procedure from the beginning. The algorithm for the groups X where $X/O_p(X) \cong {}^3D_4(q)$ or $G_2(q)$ is similar to the previous algorithm.

4.3 Estimates

In this section, we estimate the probability of producing an involution i which guarantees the construction of a long root $\mathrm{SL}_2(q)$-subgroup in a finite simple group G of Lie type of odd characteristic by the first run of Algorithm 4.1 applied to $C_G(i)$. To guarantee the success of Algorithm 4.1, we assume

that the semisimple socles of the centralizers of involutions are constructed in the recursive steps. The estimates in some cases are very crude and on the cautious side, the actual probabilities of success are much bigger.

Let $n = 2^k m$, m odd. Then the number k is called the 2-*height* of n.

Note that to produce involutions in G we need an element of even order and the share of elements of even order is at least $1/4$ by Fact 4.3.

Assume that $G = \mathrm{PSL}_n(q)$ and i is an involution of type $t'_{n/2}$. Note that such an involution exists in G if and only if n is even and 2-height of $q-1$ is bigger than the 2-height of n, see Table 2.5 and Table 4.5.1 in [25]. The semisimple socle of $C_G(i)$ is

$$\frac{1}{(n/2, q-1)}\mathrm{SL}_{n/2}(q^2).$$

If an involution of type $t'_{n/2}$ constructed in one of the recursive steps, then we obtain a subgroup $\mathrm{SL}_2(q^{2^k})$ for some $k > 1$ which is not a long root $\mathrm{SL}_2(q)$-subgroup in G. Note that an involution of type $t'_{n/2}$ belongs only in a maximal twisted torus T, twisted by the longest cycle w in the Weyl group $W = \mathrm{Sym}(n)$, symmetric group on n letters. Therefore $i = \mathrm{i}(g)$ where g is an element from a maximal twisted torus. The number of maximal twisted tori in G is $|G : N_G(T)|$. Now $|N_G(T) : T| = |C_W(w)|$ by Theorem 2.16 and $|C_W(w)| = n$ since w is a cycle of length n in W. Hence there are at most

$$\frac{|G|}{|N_G(T)|} = \frac{|G|}{|C_W(w)| \cdot |T|} = \frac{|G|}{n|T|}$$

such elements produce involutions of type $t'_{n/2}$. Therefore the probability of producing an involution of type $t'_{n/2}$ is at most $1/n$. Notice that the probability of producing such involutions in the case of central product $\mathrm{SL}_k(q) \circ \mathrm{SL}_l(q)$ is close to 0 as the elements in both components must belong to same type of torus and have the same 2-height in order to produce such an involution. Therefore if we have an involution of type different than $t'_{n/2}$ in the first step, which is of probability at least $1/4(1 - 1/n)$, we will obtain a long root $\mathrm{SL}_2(q)$-subgroup.

Assume that $G = \mathrm{PSp}_{2n}(q)$ and $q \equiv 1 \bmod 4$. Let i be an involution of type t_n, then $C_G(i) = \frac{1}{(2,n)}\mathrm{GL}_n(q)$. If we construct an involution of type t_n in one of the recursive steps, then Algorithms 4.2 and 4.12 do not return a long root $\mathrm{SL}_2(q)$-subgroup [32]. The rest is similar to the $\mathrm{PSL}_n(q)$ case. Involutions of type t_n belongs only to a maximal twisted torus T. The number

of maximal twisted tori in G is $|G : N_G(T)|$ and $|N_G(T) : T| = |C_W(w)| = 2n$ since T corresponds to a longest cycle w in the Weyl group $W = Z_2 \wr \mathrm{Sym}(n)$. Hence there are at most

$$\frac{|G|}{2n|T|}$$

elements which can produce involutions of type t_n. Therefore the probability of producing an involution of type t_n is at most $1/2n$. Hence we can produce an involution which is not of type t_n with probability at least $1/4(1-1/2n)$. If $q \equiv -1 \bmod 4$, then $C_G(i) = \frac{1}{(2,n)}\mathrm{GU}_n(q)$ for an involution of type t_n and the same arguments apply.

Assume that $G = \Omega_{2n+1}(q)$, $n \geqslant 3$. A short root $\mathrm{SL}_2(q)$-subgroup is isomorphic to $\Omega_3(q) \cong \mathrm{PSL}_2(q)$. Let i be an involution of type t_n, then $C_G(i)'' \cong \Omega^{\varepsilon}_{2n}(q)$ where $q^n \equiv \varepsilon \bmod 4$. Note that only maximal twisted tori whose order is $1/2(q^n \pm 1)$ contain involutions of type t_n, see Table 2.5. Since the Weyl groups of $\Omega_{2n+1}(q)$ and $\mathrm{PSp}_{2n}(q)$ are same, we will obtain the same estimate that we will construct $\Omega^{\varepsilon}_{2n}(q)$ as a centralizer of an involution with probability at least $1/2n$ in the first step of the algorithm. Therefore a crude estimate in this case follows from an estimate in $\mathrm{P}\Omega^{\varepsilon}_{2n}(q)$.

Assume that $G = \mathrm{P}\Omega^{\varepsilon}_{2n}(q)$, $n \geqslant 4$. If we construct $\frac{1}{2}\mathrm{SL}^{\varepsilon}_n(q)$ as a centralizer of an involution, then a lower bound for the probability of constructing long root $\mathrm{SL}_2(q)$-subgroup follows from the $\mathrm{PSL}_n(q)$-case. The desired involution is of type t_n or t'_n. Again these involutions belong to a maximal twisted tori. The probability of obtaining such involution is at least $1/2n$ by using the same ideas above and the overall probability is $1/4(1-1/n)(1/2n)$.

Assume that $G = F_4(q)$. If we have an involution i of type t_4, then $C_G(i)'' \cong \mathrm{Spin}_9(q)$ and the estimate for constructing a long root $\mathrm{SL}_2(q)$-subgroup follows from the estimate for $\Omega_9(q)$. An involution of type t_4 belongs to a torus T where T corresponds to an element $w \in W$ with $|C_W(w)| = 8$ [18, Table 4].

Let $G = E_8(q)$ or $E_7(q)$, then the possible semisimple socles for centralizers of involutions are either central products of classical groups or contain $E_7(q)$ or $E_6(q)$ respectively. In the case of central products of classical groups, we refer to the above estimates. Similarly, we reduce the estimates to $E_6(q)$ for the groups $E_7(q)$. The estimates for the groups $E_6(q)$ and ${}^2E_6(q)$ can be computed again from the estimates for classical groups as the possible semisimple socles of the centralizers of invoutions are central products of classical groups, see Table 2.5.

In $G_2(q)$ or ${}^3D_4(q)$, we can construct a long root $\mathrm{SL}_2(q)$-subgroup without any difficuilty, see Section 4.1.4.

Chapter 5

Recognition of the p-core

In this chapter we present an algorithm which determines whether $O_p(X) \neq 1$, where $X/O_p(X)$ is a finite simple classical group or unisingular group G of Lie type of odd characteristic p. In Section 5.1, we present an algorithm which was proposed by Babai and Shalev [10] and was designed for the groups when G is so-called *unisingular simple groups of Lie type of characteristic p*. It appears that the problem is much easier for the groups in this class than in general. In Section 5.2, we present an algorithm in the case where G is any classical group.

5.1 Easy case: Unisingular groups of Lie type

In this section, we present the algorithm in [10]. Let G be a finite simple group of Lie type defined over $\mathbb{F}_q$ of characteristic p. If the order of an element $g \in G$ is divisible by p, then it is called *p-singular*, otherwise we say that g is *p-regular*. Let $\rho_p(G)$ denote the proportion of p-singular elements and $s(G)$ denote the proportion of regular semisimple elements in G. Setting $\rho'_p(G) = 1 - s(G)$, then we have $\rho'_p(G)$ is the proportion of elements which commute with an element of order p.

The p-singular elements are crucial in recognizing finite simple groups of Lie type of characteristic p. However it is very difficult to find a p-singular element when q is large, namely we have

Fact 5.1. [28] *Let G be a finite simple group of Lie type of characteristic p defined over $\mathbb{F}_q$. Then*

$$\rho_p(G) \leqslant \rho'_p(G) \leqslant \frac{3}{q-1} + \frac{2}{(q-1)^2}.$$

It is clear that for any finite group X and $A \trianglelefteq X$, we have

$$\rho_p(X) \geqslant \rho_p(X/A).$$

If the quantity $\rho_p(X) - \rho_p(X/A)$ is *non-negligible* then random sampling and checking for p-singularity will work in X. It turns out below that when X/A is a finite simple unisingular group of Lie type defined over $\mathbb{F}_q$, $A = O_p(X)$ and q is big, then $\rho_p(X) - \rho_p(X/A)$ is close to 1.

Definition 5.2. *Let G be a finite simple group of Lie type of characteristic p.*

1. *Let A be any abelian p-group with a G-action. Any element $g \in G$ is said to be unisingular if g has a non-zero fixed point on A.*

2. *G is called unisingular if every element of G acts unisingularly on every finite abelian p-group A with a G-action.*

It is essential to study the unisingular action of p-regular elements by Fact 5.1.

Let

$$\lambda(A_G) = \frac{|\ p'\text{-elements in } G \text{ which are unisingular on } A\ |}{|\ G\ |}.$$

Then a simple group G of Lie type of characteristic p is unisingular if and only if

$$\lambda(A_G) = 1 - \rho_p(G) \tag{5.1}$$

for every nontrivial G-module A_G of characteristic p. Hence we have

$$\lambda(A_G) > 1 - \frac{3}{q-1} - \frac{2}{(q-1)^2}. \tag{5.2}$$

Fact 5.3. [Proposition 3.6 in [10]] *Let A be an abelian p-group, X a finite group and $\phi : X \to G$ be a epimorhism with $ker(\phi) = A$. Let $g \in G$ be p-regular.*

1. *If g is not unisingular in its action on A then all elements of $\phi^{-1}(g)$ are p-regular.*

2. *If g is unisingular in its action on A then at most $1/p$ fraction of the elements of $\phi^{-1}(g)$ are p-regular.*

By Fact 5.3, it is clear that

$$\lambda(A_G)(1-1/p) \leqslant \rho_p(X) - \rho_p(X/A) \leqslant \lambda(A_G). \tag{5.3}$$

By Equations 5.2 and 5.3, we have

$$(1 - \frac{3}{q-1} - \frac{2}{(q-1)^2})(1-1/p) < \rho_p(X) - \rho_p(X/A). \tag{5.4}$$

Algorithm 5.4. "Recognition of the p-core: The easy case"

Input: A black box group X where $X/O_p(X)$ is a finite simple unisingular groups of Lie type of characteristic p.

Output: An element from $O_p(X)$ or the statement "Probably, $O_p(X) = 1$".

Description of the algorithm:
Let $E = mp^k$ where $(m, p) = 1$. We produce a random element $x \in X$ and check whether $y = x^m \neq 1$. If $y \neq 1$, then we construct $\langle y^X \rangle$ and we check whether it is a p-group or not. If we find an element $z \in \langle y^X \rangle$ satisfying $z^{p^k} \neq 1$, then we conclude that $y \notin O_p(X)$. If we can not find such an element, then we deduce that $y \in O_p(X)$.

The probability that we fail to find a p-singular element is $(1 - \rho_p(X) + \rho_p(X/O_p(X)))^l$ where l is the number of repetitions. By Equation 5.4, we have

$$(1 - \rho_p(X) + \rho_p(X/O_p(X)))^l \leqslant O(1/p)^l.$$

Therefore when p is large, $l = 1$ suffices to find p-element in $O_p(X)$ with a big probability.

The complete list of finite simple unisingular groups of Lie type of characteristic p is as follows.

Fact 5.5. **[29]** *Let G be a finite simple group of Lie type of characteristic p defined over the field $GF(q)$, where $q = p^k$ for some $k \geqslant 1$. Then G is unisingular if and only if G is one of the following:*

1. $\mathrm{PSL}_n^{\varepsilon}(p)$ *with* $n|(p-\varepsilon)$;
2. $\mathrm{P}\Omega_{2n}^{\varepsilon}(p)$ *with p odd and* $\varepsilon = (-1)^{n(p-1)/2}$;
3. ${}^2G_2(q)$, $F_4(q)$, ${}^2F_4(q)$, $E_8(q)$ *with q arbitrary;*

4. $G_2(q)$ *with* q *odd;*

5. $E_6^\varepsilon(p)$ *with* $3|(p-\varepsilon)$*;*

6. $E_7(p)$ *with* p *odd.*

5.2 General case

Our algorithm in the general case is recursive. We reduce the problem of finding a p-element in X to the centralizers of involutions in X. The last step of the recursion deals with a group $Y \leqslant X$ where $Y/O_p(Y) \cong \mathrm{PSL}_2(q)$. In order for this procedure to work, we make use of long root $\mathrm{SL}_2(q)$-subgroups in X.

5.2.1 Pairs of long root $\mathrm{SL}_2(q)$-subgroups

In this section, we determine the subgroups generated by the two conjugate long root $\mathrm{SL}_2(q)$-subgroups in a finite simple classical group of odd characteristic.

Lemma 5.6. *Let* $G = \mathrm{PSL}_n(q)$*,* $n \geqslant 5$*. Let* $K \leqslant G$ *be a long root* $\mathrm{SL}_2(q)$*-subgroup and* $g \in G$ *be a random element. Then* $\langle K, K^g\rangle = \mathrm{SL}_4(q)$ *with probability at least* $1 - 1/q^{n-3}$*.*

Proof. Let V be a natural module for $\mathrm{SL}_n(q)$ and $V = U \oplus W$ where K induces $\mathrm{SL}_2(q)$ on U and fixes W. Assume that $U = \langle u_1, u_2\rangle$. Let $g \in \mathrm{SL}_n(q)$ and

$$gu_1 = a_1u_1 + a_2u_2 + w_1$$

$$gu_2 = b_1u_1 + b_2u_2 + w_2$$

where a_i, b_i, $i = 1, 2$, are elements in the base field and w_1, $w_2 \in W$. Observe that the vectors w_1 and w_2 are linearly dependent with probability $1/q^{n-3}$. Therefore the probability that $\dim\langle U, gU\rangle = 4$ is at least $1 - 1/q^{n-3}$. □

Lemma 5.7. *Let* $G = \mathrm{PSp}_{2n}(q)$*,* $n \geqslant 3$*. Let* $K \leqslant G$ *be a long root* $\mathrm{SL}_2(q)$*-subgroup and* $g \in G$ *be a random element. Then* $\langle K, K^g\rangle = \mathrm{Sp}_4(q)$ *with probability at least* $1 - 1/q$*.*

Proof. Let V be the natural module for $\mathrm{Sp}_{2n}(q)$ and $V = V_1 \perp \ldots \perp V_n$ be an orthogonal decomposition of V where V_k is a hyperbolic plane for each $k = 1, \ldots, n$. Assume that $V_k = \langle e_k, f_k \rangle$ where $\{e_k, f_k\}$ are hyperbolic pairs. We may assume that $K = \mathrm{Sp}(V_1)$. Let $g \in \mathrm{Sp}_{2n}(q)$ and V_1' be the natural module for K^g. It is clear that V_1' is hyperbolic plane in V. The probability that the space $\langle V_1, V_1' \rangle$ is non-degenerate 4-space is

$$A(B - C)/D,$$

where A is the number of non-degenerate 4-spaces, U_4, of V containing V_1, B is the number of hyperbolic planes in U_4, C is the number of hyperbolic planes in U_4 intersecting non-trivially with V_1 and D is the number of hyperbolic planes in V. By the computation in [2, Chapter 3], there are $(q^{2n-2}(q^{2n} - 1))/(q^2 - 1)$ distinct hyperbolic planes in a $2n$-dimensional non-degenerate symplectic geometry, and there are $q^2(q+1)$ hyperbolic planes in U_4 intersecting non-trivially with V_1. Hence the the probability that $\langle V_1, V_1' \rangle$ is a 4-dimensional symplectic geometry with probability at least

$$\frac{q^{2n-4}(q^{2n-2} - 1)\{(q^2(q^2 + 1) - q^2(q + 1))\}}{q^{2n-2}(q^{2n} - 1)} > 1 - 1/q.$$

□

Lemma 5.8. *Let $G = \mathrm{P}\Omega^{\pm}(V)$ be a simple orthogonal group with $\dim V \geqslant 9$. Let $K \leqslant G$ be a long root $\mathrm{SL}_2(q)$-subgroup and $g \in G$ be a random element. Then $\langle K, K^g \rangle = \Omega_8^+(q)$ with probability at least $(1 - 1/q)^2$.*

Proof. Let V be the natural module for $\Omega^{\pm}(V)$. Then

$$[K, V] = \langle kv - v \mid v \in V,\, k \in K \rangle$$

is a orthogonal 4-space of Witt index 2 and let $U = [K, V] = \langle e_1, e_2, f_1, f_2 \rangle$ where $\{e_i, f_i\}$ are hyperbolic pairs. Let $U' = \langle e_1', e_2', f_1', f_2' \rangle \leqslant V$ be the othogonal 4-space of Witt index 2 on which K^g induces $\mathrm{SL}_2(q)$ for $g \in \Omega^{\pm}(V)$. Again by computation in [2, Chapter 3], there are

$$\begin{array}{cc} q^{n-2}(q^{n-1} - 1) & \text{if } n \text{ is odd,} \\ q^{n-2}(q^{n/2} - 1)(q^{n/2-1} + 1) & \text{if } n \text{ is even and } G = \mathrm{P}\Omega^+(V), \\ q^{n-2}(q^{n/2} + 1)(q^{n/2-1} - 1) & \text{if } n \text{ is even and } G = \mathrm{P}\Omega^-(V) \end{array}$$

total number of hyperbolic pairs. By the similar computations as in Lemma 5.7, the subspace $U_1 = \langle U, e_1', f_1' \rangle$ is a non-degenerate 6-space with Witt index 3 and the subspace $\langle U_1, e_2', f_2' \rangle$ is a non-degenerate 8-space with Witt index 4 with probability at least $1 - 1/q$. Hence $\langle U, gU \rangle$ is a orthogonal 8-space with Witt index 4 with probability at least $(1 - 1/q)^2$. □

Lemma 5.9. *Let $G = \mathrm{PSU}_n(q)$, $n \geqslant 5$. Let $K \leqslant G$ be a long root $\mathrm{SL}_2(q)$-subgroup and $g \in G$ be a random element. Then $\langle K, K^g \rangle = \mathrm{SU}_4(q)$ with probability at least $1 - O(1/q)$.*

Proof. Similar to the arguments above.

Lemma 5.10. *Let $G = (\mathrm{P})\mathrm{SL}_n(q)$, $(\mathrm{P})\mathrm{SU}_n(q)$, $n = 2, 3, 4$, or $(\mathrm{P})\mathrm{Sp}_4(q)$, $\Omega_7(q)$, $\Omega_8^{\pm}(q)$ and K be a long root $\mathrm{SL}_2(q)$-subgroup in G, then $\langle K, K^g \rangle = G$ with probability at least $1 - O(1/q)$.*

Proof. Similar to the arguments above.

5.2.2 An algorithm for classical groups

We shall use the function ζ_1^i for generating the centralizers of involutions $i \in X$. In our algorithm, we use only classical involutions. Therefore it is enough to obtain a lower bound for the probability that ii^g has odd order for only classical involutions $i \in G$.

Theorem 5.11. *Let G be a finite simple classical group over a field of odd characteristic p and $i \in G$ be a classical involution. Then the product ii^g has odd order with probability bounded from below by constant which does not depend on G.*

Proof. Let $i \in G$ be a classical involution, then it belongs to some long root $\mathrm{SL}_2(q)$-subgroup $K \leqslant G$. Therefore, the product ii^g belongs to the subgroup $L = \langle K, K^g \rangle$. We have shown in Section 5.2.1 that the subgroup L has a given structure depending on G with probability at least $1/2$. Hence it is enough to find the probability that a product of two conjugate classical involutions in L has odd order.

Consider the map

$$\begin{aligned} \varphi : i^L \times i^L &\to L \\ (i^g, i^h) &\mapsto i^g i^h. \end{aligned}$$

Take a torus $T \leqslant L$ inverted by $j = i^{g'}$ for some $g' \in L$, that is, satisfying $t^j = t^{-1}$ for all $t \in T$. Let $x \in T$ be an element of odd order. Then there exists $h \in \langle x \rangle$ such that $h^2 = x$. Now

$$jj^h = jh^{-1}jh = hh = x$$

since j inverts T. Hence elements of odd order in T are in the image of φ. Let $x \in T$ be a regular element, that is, $C_L(x) = T$, which has odd order. Then $|\varphi^{-1}(x)| \geqslant |T|$ since $j^t j^{ht} = (jj^h)^t = (hh)^t = x^t = x$ for any $t \in T$. Let S be the set of regular elements in T which are of odd order. Let R be the set of all regular elements in L whose elements are conjugate to elements in S, then

$$|R| = |L : N_L(T)||S|.$$

Now observe that

$$|\varphi^{-1}(R)| \geqslant |R||S|,$$

and

$$|i^L \times i^L| = \frac{|L|^2}{|C_L(i)|^2}.$$

Therefore the share of pairs of involutions which are mapped to R is

$$\frac{|\varphi^{-1}(R)|}{|i^L \times i^L|} \geqslant \frac{|R||S||C_L(i)|^2}{|L|^2} = \frac{|S|^2|C_L(i)|^2}{|N_L(T)||L|}.$$

Now, we shall find a lower bound to this quotient in all finite simple classical groups.

Let $G = \mathrm{PSL}_n(q)$, $n \geqslant 5$. Then $L = \mathrm{SL}_4(q)$ with probability at least $1/2$ by Lemma 5.6. Observe that a classical involution $i \in L$ inverts a cyclic torus $H \leqslant L$ of order $q^2 + 1$ and $(q^2 + 1)/2$ is an odd number. Observe also that H is uniquely contained in a maximal cyclic torus $T \leqslant L$ of order $(q + 1)(q^2 + 1) = (q^4 - 1)/(q - 1)$. Note that the maximal torus T in L corresponds to a 4-cycle in the Weyl group of L which is $Sym(4)$ in this case. Hence $|R| \geqslant \frac{|L|}{8(q+1)}$, $|S| \geqslant (q^2 + 1)/2$, $|C_L(i)| = q^2(q^2 - 1)^2(q - 1)$ and $|L| = q^6(q^2 - 1)(q^3 - 1)(q^4 - 1)$. After a simple rearrangement

$$\frac{|\varphi^{-1}(R)|}{|i^L \times i^L|} \geqslant \frac{(q - 1)^3(q + 1)}{16q^2(q^2 + q + 1)} \geqslant \frac{1}{32}.$$

Hence $ii^g \in \mathrm{PSL}_n(q)$ is of odd order with probability at least $1/64$. If $G = (\mathrm{P})\mathrm{SL}_n(q)$, $n \leqslant 4$, then $L = G$ with probability at least $1/2$ by Lemma 5.6, and by the same computations we obtain a similar result.

Let $G = \mathrm{PSp}_{2n}(q)$, $n \geqslant 3$. Then $L = \mathrm{Sp}_4(q)$ with probability at least $1/2$ by Lemma 5.7. The classical involutions invert a tori of order $q \pm 1$. Let $T \leqslant L$ be a torus of order $q-1$ inverted by a classical involution $i \in L$ and $q \equiv -1 \mod 4$, then $(q-1)/2$ is an odd number. Observe that $C_L(T) \cong \mathrm{GL}_2(q)$ and $|N_L(T)/C_L(T)| = 2$, $C_L(i)$ is isomorphic to $\mathrm{SL}_2(q) \times \mathrm{SL}_2(q)$. Now after a simple rearrangement, we have

$$\frac{|\varphi^{-1}(R)|}{|i^L \times i^L|} \geqslant \frac{1}{4}\frac{(q-1)^2(q+1)}{q(q^2+1)} \geqslant 1/16.$$

Hence $ii^g \in \mathrm{PSp}_{2n}(q)$ is of odd order with probability at least $1/32$. If $q \equiv 1 \mod 4$, then we consider tori of order $q+1$. If $G = \mathrm{PSp}_4(q)$, then $L = G$ with probability at least $1/2$ by Lemma 5.7 and by the same arguments we obtain a similar result.

Let $G = \Omega_8^-(q)$, then $L = G$ with probability at least $1/2$ by the computations in Section 5.2.1. Observe that the classical involutions $i \in G$ inverts a maximal torus T of order $(q^4+1)/2$ which is an odd number. Now, $|C_G(i)| = \frac{1}{4}q^4(q-1)^3(q+1)^3(q^2+1)$, $|S| \geqslant (q^4+1)/2$, $|N_G(T)/T| = 12$. Hence

$$\frac{|\varphi^{-1}(R)|}{|i^L \times i^L|} \geqslant \frac{1}{384}\frac{(q-1)^4(q+1)^4(q^2+1)}{q^4(q^6-1)} \geqslant \frac{1}{1536}.$$

Hence $ii^g \in \Omega_8^-(q)$ is of odd order with probability at least $1/(2 \cdot 1536) = 1/3072$.

Assume now that $G = \Omega_8^+(q)$ or $\Omega_n^\varepsilon(q)$, $n \geqslant 9$, then $L \cong \Omega_8^+(q)$ with probability at least $1/2$ by Lemma 5.8. Observe that L contains a subgroup of the form $N = \Omega_4^-(q) \times \Omega_4^-(q)$, and there is an involution $i \in \Omega_4^-(q)$ which inverts a torus of order $(q^2+1)/2$. Notice that i is necessarily an involution of type t_1 in L, see Table 2.5. Now the involution $j = (i,i) \in N$ inverts a torus T of order $(q^2+1)^2/4$ which is an odd number. Since j is a product of two commuting involution of type t_1, it is of type t_2 in L and therefore it is a classical involution. Hence

$$|S| \geqslant (q^2+1)^2/4,$$

$$|C_L(i)| = 4|\Omega_4^+(q)|^2 = q^4(q-1)^4(q+1)^4,$$
$$|L| = q^{12}(q^4-1)(q^2-1)(q^4-1)(q^6-1),$$
$$|N_L(T)| = 8(q^2+1)^2,$$

and

$$\frac{|\varphi^{-1}(R)|}{|i^L \times i^L|} \geqslant \frac{q^8(q-1)^8(q+1)^8(q^2+1)^4}{128(q^2+1)^2(q^{12}(q^4-1)(q^2-1)(q^4-1)(q^6-1))}.$$

After a simple rearrangement we have

$$\frac{|\varphi^{-1}(R)|}{|i^L \times i^L|} \geqslant \frac{(q^2-1)^5}{128q^4(q^6-1)} \geqslant \frac{1}{128 \cdot 6} = \frac{1}{768}.$$

□

Lemma 5.12. *Let X be a finite group, $i \in X$ an involution and $Q = O_p(X)$. If $C_Q(i) = 1$ then $\bar{i} \in Z(\bar{X})$ where $\bar{X} = X/QC_X(Q)$.*

Proof. Notice that $i \in X$ inverts Q, that is, $x^i = x^{-1}$ for any $x \in Q$ and Q is abelian. Now $[i, x] \in QC_X(Q)$ for all $x \in X$ and the result follows. □

Let $X/O_p(X) \cong \mathrm{PSL}_2(q)$ and $i \in X$ be an involution. Assume that $Q = O_p(X) \neq 1$. It is easy to see that $C_Q(i) \neq 1$ by Lemma 5.12 and therefore $O_p(C_X(i)) \neq 1$. Now $C_X(i)/O_p(C_X(i))$ is isomorphic to a dihedral group of order $q \pm 1$. Let $Q_1 = O_p(C_X(i))$. If $O_p(C_X(i)') = 1$, then random elements in $C_X(i)$ have orders which are multiple of p and we can find a p-element in Q_1 by raising a random element in $C_X(i)$ to the power $q \pm 1$. Hence we can assume that $O_p(C_X(i)') \neq 1$. Now $C_X(i)'/O_p(C_X(i)')$ is isomorphic to a cyclic group of order $(q \pm 1)/2$. Hence when we take the power $(q \pm 1)/2$ of random elements in $C_X(i)'$ we can produce p-elements in $O_p(C_x(i)')$ and we are done. Our approach in the general case is to reduce to problem to this case in all finite simple classical groups. The structure of the algorithm is as follows.

Algorithm 5.13. "Recognition of the p-core"

> *Input: A black box group X with the property that $X/O_p(X)$ is a finite simple classical group of odd characteristic p.*
>
> *Output: If $O_p(X) \neq 1$, then the algorithm finds a non-trivial p-element in $O_p(X)$ with probability bounded from below by a constant. Otherwise it returns the statement "Possibly, the p-core is trivial".*

Description of the algorithm:
Step 0: Check whether random search works in X.

In this step, we use Algorithm 5.4, see Section 5.1.

Step 1: Construct $K \leqslant X$ where $K/O_p(K)$ is a long root $\mathrm{SL}_2(q)$-subgroup in $X/O_p(X)$ and check whether $O_p(K) \neq 1$.

We will use Algorithm 4.18 to construct K. In each recursive step in the construction of K, we check whether random search works as in Step 0. Note that in the construction of K we are using the function ζ_0^i as well as ζ_1^i for the involutions $i \in X$. Therefore if we are in the situation of using only the function ζ_0^i in some recursive steps, $O_p(K)$ may be trivial even though $O_p(X) \neq 1$. We check whether $O_p(K) \neq 1$ as above, namely if $O_p(K) \neq 1$, then $K/\langle i \rangle$ is isomorphic to $\mathrm{PSL}_2(q)$ extended by some p-group and we apply the above procedure. If we can not find a p-element then we go to next step.

Step 2: Construct $C_X(i)$ by using ζ_1^i, and $C_X(i)''$ where $i \in K$ is an involution.

We construct the involution $i \in K$. Note that $i \in Z(K)$. By Facts 3.1 (a) and 4.5, the image of the function ζ_1^i for reasonable number of sample elements generates $C_X(i)$ with probability close to 1, and the share of elements for which the map ζ_1^i is defined is bounded from below by constant by Theorem 5.11. To construct the derived subgroups, we use the algorithm in [8] as before.

Set $Q = O_p(X)$. If $C_Q(i) = 1$, then certain power of commutators of random elements are p-elements in $O_p(X)$ by the proof of Lemma 5.12. Therefore assume that $C_Q(i) \neq 1$ which implies that $O_p(C_X(i)) \neq 1$. Now if $O_p(C_X(i)') = 1$ or $O_p(C_X(i)'') = 1$, then certain power of random elements in $C_X(i)$ or $C_X(i)'$ are p-elements in $O_p(X)$ respectively. Recall that, by Corollary 2.19, $C_X(i)''/O_p(C_X(i)'')$ is a product of quasi-simple groups. Therefore if p-elements can not be found by powering random elements in $C_X(i)''$, then we go to next step.

Step 3: Construct 2-components K_1'' and L_1'' of $C_X(i)''$.

By Corollary 2.19 and Corollary 2.20, $C_X(i)$ has a 2-component K_1 where $K_1/O_p(K_1)$ is a long root $\mathrm{SL}_2(q)$-subgroup in $X/O_p(X)$. The other 2-component(s) L_1 in $C_X(i)$ can be read from Table 2.6.

Assume that $G = \mathrm{PSL}_n(q)$, $\mathrm{PSU}_n(q)$, $\mathrm{PSp}_{2n}(q)$, $\Omega_{2n+1}(q)$ or $\mathrm{P}\Omega^{\pm}_{2n}(q)$, then $C_G(i)'' = K_1L_1$ for a classical involution $i \in G$ and $L_1 = \mathrm{SL}_{n-2}(q)$, $\mathrm{SU}_{n-2}(q)$, $\mathrm{Sp}_{2n-2}(q)$, $\mathrm{SL}_2(q)\Omega_{2n-3}(q)$ or $\mathrm{SL}_2(q)\Omega^{\pm}_{2n-4}(q)$ respectively.

Consider the following tori in a classical group L_1.

G	L_1	$\lvert T\rvert$
$\mathrm{PSL}_n(q)$	$\mathrm{SL}_{n-2}(q)$	$\{\begin{smallmatrix}(q^{n-2}-1)/(q-1),\\ q^{n-3}-1\end{smallmatrix}$
$\mathrm{PSU}_n(q)$	$\mathrm{SU}_{n-2}(q)$	$(q^{n-2}-(-1)^{n-2})/(q+1)$
$\mathrm{PSp}_{2n}(q)$	$\mathrm{Sp}_{2n-2}(q)$	$(q^{n-1}+1)/2$
$\mathrm{P}\Omega_{2n+1}(q)$	$\Omega_{2n-3}(q)$	$(q^{n-2}+1)/2$
$\mathrm{P}\Omega^+_{2n}(q)$	$\Omega^+_{2n-4}(q)$	$(q^{n-3}+1)(q+1)/2$
$\mathrm{P}\Omega^-_{2n}(q)$	$\Omega^-_{2n-4}(q)$	$(q^{n-2}+1)/2$

In order to construct K_1 in the commuting product $C = C_G(i)''$, we construct a non-central element $g \in C$ of order dividing $q \pm 1$. Then we construct $H = \langle g^C \rangle'$ and we check whether H is isomorphic to $\mathrm{SL}_2(q)$ by just raising some random elements to the power $q(q^2-1)$ and compare with identity.

Note that maximal tori considered above are conjugate in the corresponding groups and they correspond to elements $w \in W$ where the order $C_W(w)$ is $O(n)$, see Theorem 2.15. Since $|N_G(T)/T| \cong |C_W(w)|$ by Theorem 2.16, the probability that a random element belongs to a torus conjugate to T is $O(1/n)$.

Let $L_1 = \mathrm{SL}_{n-2}(q)$. If n is even, then $((q^{n-3}-1), q+1) = 2$ and we consider a torus of order $q^{n-3}-1$. If n is odd, then $((q^{n-2}-1)/(q-1), q+1) = 1$ and we consider a torus of order $(q^{n-2}-1)/q-1$. Note that the probability that an element in L_1 having an order dividing $(q^{n-2}-1)/(q-1)$ or $q^{n-3}-1$ is at least $1/(n-2)$ or $1/(n-3)$ respectively, see Section 4.3 for such computations. Therefore with probability at least $1/(n-3)$, $h = g^{E/(q+1)^a} \in K_1$ where E is an exponent for G and a is the biggest power of $(q+1)$ in E. If h is a central element in C then we repeat this proces until we get a non-central element. The process of checking whether h is central or not in C is to check whether h commutes with each generator of C. Now it is clear that $\langle h^C \rangle' = K_1$.

In the rest of the cases observe that $(|T|, q-1) = 2$ except $L_1 = \mathrm{SU}_{n-2}(q)$ and n is even in which case we consider the torus T of order $(q^{n-3}+1)$. Therefore after $O(n)$ iterations we can find an element $g \in C$ such that $h = g^{E/(q-1)^b}$ is a non-central element in K_1 where b is the maximal power of $q-1$ in E and hence $\langle h^C \rangle' = K_1$.

It is easy to see that the above argument can be applied to the groups with non-trivial p-core in construction of K_1. Now we check whether K_1 has non-trivial p-core as before. If $O_p(K_1) = 1$, then we construct L_1'' by raising the power $q(q^2-1)$ of the elements in the generating set for $C_X(i)''$. If L_1'' is a commuting products of (P)$\mathrm{SL}_2(q)$, then we use the idea in Algorithm 4.12 to construct each (P)$\mathrm{SL}_2(q)$ in L_1''.

Step 4: Set $X = L_1''$. Go to Step 1.

If $O_p(X) \neq 1$ and $O_p(K_1'') = 1$, then $O_p(L_1'') \neq 1$. Therefore we set $X = L_1''$ and go to Step 1. Here we recursively construct subgroups K_s, $s \geqslant 1$ where $K_s/O_p(K_s)$ is centrally isomorphic to $\mathrm{PSL}_2(q)$ for each s. If we fail to construct p-elements in all these subgroups, we conclude that $O_p(X) = 1$.

Chapter 6

Construction of Curtis - Phan - Tits system in black box groups

Finite groups of Lie type have a special presentation called the *Steinberg-presentation* which is based on the relations on its root subgroups.

Let G be a universal untwisted group of Lie type of rank $n \geqslant 2$ defined over $\mathbb{F}_q$, Σ its roots system and X_α root subgroups for $\alpha \in \Sigma$. Then $G = \langle X_\alpha \mid \alpha \in \Sigma \rangle$ and X_α is isomorphic to additive group of $\mathbb{F}_q$ where

$$X_\alpha = \{x_\alpha(t) \mid t \in \mathbb{F}_q\}$$

and

$$x_\alpha(t+u) = x_\alpha(t)x_\alpha(u). \tag{6.1}$$

The following equation is known as the Chevalley commutator formula.

$$[x_\alpha(t), x_\beta(u)] = \prod_\gamma x_\gamma(c_{i,j,\alpha,\beta}t^i u^j) \tag{6.2}$$

where $\alpha,\ \beta \in \Sigma$, $\alpha \neq \pm\beta$ and γ runs over all roots of Σ of the form $\gamma = i\alpha + j\beta$ with i, j positive integers. The coefficients $c_{i,j,\alpha,\beta}$ are integers in $[-3, 3]$ and they are independent of n and q. The group G also satisfies

$$h_\alpha(t)h_\alpha(u) = h_\alpha(tu) \quad tu \neq 0 \tag{6.3}$$

where

$$h_\alpha(t) = n_\alpha(t)n_\alpha(-1),$$
$$n_\alpha(t) = x_\alpha(t)x_{-\alpha}(-t^{-1})x_\alpha(t).$$

Fact 6.1. [Theorem 8 in [47]] *Let Σ be an irreducible root system of rank at least 2 and K be a finite field. For each root $\alpha \in \Sigma$ and $t \in K$ introduce*

a symbol $\bar{x}_\alpha(t)$. Let $\bar{G}$ be a finite group generated by the elements $\bar{x}_\alpha(t)$ with respect to the relations in Equations 6.1, 6.2 and 6.3. Then $\bar{G}/Z(\bar{G})$ is isomorphic to the finite simple group of Lie type over K having root system Σ.

Remark 6.2. The analogue of Fact 6.1 holds also for twisted groups of Lie type but the Chevalley commutator formula is more complicated, a detailed discussion can be found in [25, Section 2.4, 2.9].

The following theorem (known as the Curtis-Tits presentation) shows that the essential relations in the Steinberg presentation are the ones involving rank 1-subgroups corresponding to fundamental roots. Note that we have

$$\langle X_\alpha, X_{-\alpha}\rangle \cong (\mathrm{P})\mathrm{SL}_2(q)$$

for any $\alpha \in \Sigma$ for untwisted G (cf. Table 2.4). Note also that the nodes in the Dynkin diagram are labelled by the elements in Π. Therefore the Curtis-Tits presentation involves the pairs of fundamental roots which are edges or nonedges in the Dynkin diagram. More precisely;

Fact 6.3. [Theorem 2 in [48]] *Let Σ be an irreducible root system of rank at least 3 with fundamental system Π and Dynkin diagram Δ. Let G be a finite group and assume that the following are satisfied*

1. *$G = \langle K_\alpha \mid \alpha \in \Pi\rangle$, $K_\alpha = \langle X_\alpha, X_{-\alpha}\rangle = (\mathrm{P})\mathrm{SL}_2(q)$, for all $\alpha \in \Pi$.*
2. *$H_\alpha = N_{K_\alpha}(X_\alpha) \cap N_{K_\alpha}(X_{-\alpha}) \leqslant N_G(X_\beta)$ for all $\alpha, \beta \in \Pi$.*
3. *$[K_\alpha, K_\beta] = 1$ if α and β are not connnected in Δ.*
4. *$\langle K_\alpha, K_\beta\rangle \cong (\mathrm{P})\mathrm{SL}_3(q)$ if α and β are connected with a single bond.*
5. *$\langle K_\alpha, K_\beta\rangle \cong (\mathrm{P})\mathrm{Sp}_4(q)$ if α and β are connected with a double bond.*

Then there exists a group of Lie type $\widetilde{G}$ with a root system Σ and a fundamental system Π, and a surjective homomorphism $\varphi : G \to \widetilde{G}$ mapping the $X_{\pm\alpha}$ onto the corresponding fundamental root subgroups of $\widetilde{G}$. Moreover $\ker\varphi \leqslant Z(G) \cap H$ *where $H = \langle H_\alpha \mid \alpha \in \Pi\rangle$.*

Example 6.4. [Example in [47], p. 72] Let $G = \mathrm{SL}_n(q)$, $n \geqslant 3$ and $x_{ij}(t) = I + tE_{ij}$ where E_{ij} is the matrix whose (i,j)-entry is 1 and the others are 0. Then Steinberg-presentation of G is

$$G = \langle x_{ij}(t) \mid 1 \leqslant i, j \leqslant n,\, i \neq j,\, t \in \mathbb{F}_q \rangle$$

subject to the following relations

1. $x_{ij}(t+u) = x_{ij}(t)x_{ij}(u)$,
2. $[x_{ij}(t), x_{jk}(u)] = [x_{ik}(tu)]$ if i, j, k are different,
3. $[x_{ij}(t), x_{kl}(u)] = 1$ if $j \neq k$, $i \neq l$.

In the Curtis-Tits presentation of G we use only the generators $x_{ij}(t)$ where $\mid i - j \mid \leqslant 2$. Hence the number of relations is considerably less than the number of relations in Steinberg-presentation.

Phan proved similar results for the twisted groups of Lie type in [45]. Bennet and Shpectorov proved Phan's theorem with weaker assumptions for the groups $G = \mathrm{SU}_n(q)$ and we state this result.

Fact 6.5. [12] *Let G be a finite group containing subgroups $K_i \cong \mathrm{SU}_2(q)$, $i = 1, 2, \ldots, n$ and $K_{i,j}$, $1 \leqslant i < j \leqslant n$, such that the following hold:*

1. *If $\mid i - j \mid > 1$ then $K_{i,j}$ is a central product of K_i and K_j.*
2. *For $i = 1, 2, \ldots, n-1$, K_i and K_{i+1} are contained in $K_{i,i+1}$ which is isomorphic to $\mathrm{SU}_3(q)$ or $\mathrm{PSU}_3(q)$. Moreover K_i and K_{i+1} are the stabilizers of a non-singular vector in $K_{i,i+1}$.*
3. *The subgroups $K_{i,j}$, $1 \leqslant i < j \leqslant n$, generate G.*

If $q > 3$, then G is isomorphic to a factor group of $\mathrm{SU}_{n+1}(q)$.

It is easy to see that the subgroups K_i, $i = 1, 2, \ldots, n$ in Fact 6.5 play the role of the subgroups corresponding to the nodes in the Dynkin diagram of $\mathrm{PSL}_{n+1}(q)$ as in the Curtis-Tits presentation.

Now our principal aim is to develop a black box group algorithm which constructs a list of subgroups in $G = \mathrm{PSL}_n(q)$ and $\mathrm{PSU}_n(q)$ corresponding to the nodes in the extended Dynkin diagram for $\mathrm{PSL}_n(q)$. These subgroups are long root $\mathrm{SL}_2(q)$-subgroups in G. Our algorithm shall produce some generators for these subgroups.

6.1 Determination of the type

In this section, our aim is to present an algorithm which determines the type (linear, symplectic, unitary, orthogonal) of the given classical group over a field of odd order. The algorithm is based mostly on Theorem 1.1.

Algorithm 6.6. "Determination of the type"

Input: A black box group G isomorphic to a finite simple classical group of odd characteristic p.

Output: It finds the size of the underlying field, q, and returns one of the following statements:

"G is isomorphic to $\mathrm{PSL}_n(q)$ for some n"

"G is isomorphic to $\mathrm{PSU}_n(q)$ for some n"

"G is isomorphic to $\mathrm{PSp}_{2n}(q)$ for some n"

"G is isomorphic to $\mathrm{P}\Omega^{\varepsilon}_n(q)$ for some n".

Description of the algorithm:
Step1: We construct a long root $\mathrm{SL}_2(q)$-subgroup in G by using Algorithm 4.1 and find the size of the underlying field by using Algorithm 4.13.
Step2: We produce a random element $g \in G$ and determine the type of the group $L = \langle K, K^g \rangle$.

The subgroup L has similar structure with G, that is, by Lemmas 5.6, 5.7, 5.8, 5.9, the structure of the subgroup L is given in Table 6.1 which holds with probability at least $1 - O(1/q)$ for random $g \in G$;

Table 6.1: Pairs of long root $\mathrm{SL}_2(q)$-subgroups

G	condition	L
$\mathrm{PSL}_n(q)$	$n \geqslant 4$	$(\mathrm{P})\mathrm{SL}_4(q)$
$\mathrm{PSU}_n(q)$	$n \geqslant 4$	$(\mathrm{P})\mathrm{SU}_4(q)$
$\mathrm{PSp}_{2n}(q)$	$n \geqslant 2$	$(\mathrm{P})\mathrm{Sp}_4(q)$
$\mathrm{P}\Omega^{\varepsilon}_n(q)$	$n \geqslant 9$	$\Omega^{+}_8(q)$

If n is smaller than it is stated in the second column in Table 6.1, then by Lemma 5.10 we have $G = L$ with probability at least $1 - O(1/q)$ for random $g \in G$.

Assume first that the subgroup L is one of the following given in Table 6.1. We have

$$|\mathrm{SL}_4(q)| = q^6(q^2-1)(q^3-1)(q^4-1),$$
$$|\mathrm{SU}_4(q)| = q^6(q^2-1)(q^3+1)(q^4-1),$$
$$|\mathrm{Sp}_4(q)| = q^4(q^2-1)(q^4-1),$$
$$|\Omega_8^+(q)| = \frac{1}{2}q^{12}(q^4-1)(q^2-1)(q^4-1)(q^6-1).$$

Among these groups only $\Omega_8^+(q)$ has cyclic tori T of order $(q^4-1)/2$. Therefore if we find an element $g \in L$ satisfying $g^{q^4-1} = 1$ but $g^{(q^4-1)/a} \neq 1$ for a proper divisor $a > 2$ of $q^4 - 1$, then we conclude that $L = \Omega_8^+(q)$ and G is orthogonal. The probability of finding a generator of T is close to $1/\log\log q$ by [41] and the probability that an element in L conjugate to an element in T is determined by the Weyl group W of L, that is, T corresponds to an element $w \in W$ such that $|N_L(T)/T| = |C_W(w)| = 8$. Hence the probability of finding such an element in L is at least

$$\frac{1}{\log\log q}\frac{|L|}{|N_L(T)|} \cdot \frac{|T|}{|L|} = \frac{1}{8\log\log q}.$$

If we can not find such an element after a good sample of elements in L, then we deduce that $L \ncong \Omega_8^+(q)$ and hence G is not an orthogonal group with probability close to 0. Now we may assume that $L \cong (\mathrm{P})\mathrm{SL}_4(q)$, $(\mathrm{P})\mathrm{SU}_4(q)$ or $(\mathrm{P})\mathrm{Sp}_4(q)$. Set $E_1 = q^{12}(q^2-1)(q^4-1)$, $E_2 = q^{12}(q^2-1)(q^3-1)(q^4-1)$, $E_3 = q^{12}(q^2-1)(q^3+1)(q^4-1)$. Notice that if an element $g \in L$ satisfy $g^{E_1} = g^{E_2} = 1$ and $g^{E_3} \neq 1$ then $L \cong (\mathrm{P})\mathrm{SL}_4(q)$ and G is isomorphic to $\mathrm{PSL}_n(q)$ for some n. These elements have orders dividing $q^3 - 1$ but not $(q-1)(q^2-1)$. Therefore they belong to tori of order $q^3 - 1$ and at least half of the elements in these tori have orders not dividing $(q-1)(q^2-1)$. Let T be such a torus, then $|N_L(T)/T| = 3$ by the same argument above. Now, in $L = (\mathrm{P})\mathrm{SL}_4(q)$, the probability of finding such element is at least

$$\frac{|L|}{|N_L(T)|} \cdot \frac{|T|}{2|L|} = \frac{1}{6}.$$

Similarly, if an element $g \in L$ satisfy $g^{E_1} = g^{E_3} = 1$ and $g^{E_2} \neq 1$ then $L \cong (\mathrm{P})\mathrm{SU}_4(q)$ and G is isomorphic to $\mathrm{PSU}_n(q)$ for some n. These elements belong to a torus of order q^3+1, and the probability of finding such elements in $(\mathrm{P})\mathrm{SU}_4(q)$ is at least $1/6$ by the same argument above and Fact 2.16. If we always have $g^{E_1} = 1$, then we deduce that $L \cong (\mathrm{P})\mathrm{Sp}_4(q)$ and G is isomorphic to $\mathrm{PSp}_{2n}(q)$ for some n.

If $G = \mathrm{PSL}_3(q)$, $\mathrm{PSU}_3(q)$ or $\Omega_7(q)$, then $L = G$ with probability at least $1 - O(1/q)$ by Lemma 5.10. The same argument above applies to distinguish these groups.

The main corollary of Algorithm 6.6 is an algorithm which distinguishes the groups $\mathrm{PSp}_{2n}(q)$ and $\Omega_{2n+1}(q)$. Such an algorithm was first presented by Altseimer and Borovik [1]. An algorithm for distinguishing $\mathrm{PSp}_{2n}(q)$ from $\Omega_{2n+1}(q)$ is important because of the fact that the statistics of element orders are virtually the same in these two groups, see [1] for more details, hence an approach based on the analysis on the element orders do not provide an efficient algorithm [9]. The algorithm in [1] uses the structure of the centralizers of involutions and conjugacy classes in these groups but it is completely different from the one presented in Algorithm 6.6. Therefore we state this alternative algorithm.

Corollary 6.7. *Let G be a black box group isomorphic to $\mathrm{PSp}_{2n}(q)$ or $\Omega_{2n+1}(q)$, $q > 3$, q odd, $n \geqslant 3$. Then there is a one sided Monte–Carlo polynomial time algorithm which decides whether G is isomorphic to $\mathrm{PSp}_{2n}(q)$ or not.*

6.2 Construction of the Curtis-Tits system

In this section we present an algorithm which constructs Curtis-Phan-Tits system for the groups $(\mathrm{P})\mathrm{SL}^{\varepsilon}_n(q)$, $n \geqslant 3$. The following two lemmas are crucial in the construction.

Lemma 6.8. *Let $G = (\mathrm{P})\mathrm{SL}^{\varepsilon}_n(q)$, $n \geqslant 3$, $K \leqslant G$ be a long root $\mathrm{SL}_2(q)$-subgroup. Let $i \in K$ be the involution, then the probability of producing an involution $j \in C_G(i)$ by the map ζ_0^i which does not centralize K is bounded from below by the constant $1/192$.*

Proof. The proof follows the same arguments and notations in Theorem 5.11. The subgroup $\langle i, i^g \rangle$ can be embedded into a subgroup L isomorphic

to $\mathrm{SL}_4(q)$ or $\mathrm{SU}_4(q)$ for any $g \in G$ if $G = (\mathrm{P})\mathrm{SL}_n(q)$ or $(\mathrm{P})\mathrm{SU}_n(q)$, $n \geqslant 5$, respectively. Assume that $n \geqslant 5$, then it is enough to find the estimate in $\mathrm{SL}_4(q)$ and $\mathrm{SU}_4(q)$.

We count the number of elements of even order belonging to tori which are inverted by i. We consider the tori which have involutions not centralizing the components in $C_L(i)$.

Consider the map

$$\begin{aligned} \varphi : i^L \times i^L &\to L \\ (i^g, i^h) &\mapsto i^g i^h. \end{aligned}$$

Let $T \leqslant L$ be a cyclic torus inverted by $j = i^{g'}$ for some $g' \in L$. Then half of the elements of T are squares, namely half of the elements $x \in T$ satisfies $x = h^2$ for some $h \in T$ and

$$jj^h = jh^{-1}jh = hh = x$$

since j inverts T. Hence half of the elements are in the image of φ.

Let $x \in T$ be a regular element of even order. Then $|\varphi^{-1}(x)| \geqslant |T|/2$ since $j^t j^{ht} = (jj^h)^t = (hh)^t = x^t = x$ for any $t \in T$. Let S be the set of regular elements in T which are of even order and R the set of all regular elements in L whose elements are conjugate to elements in S, then

$$|R| = |L : N_L(T)||S|,$$

and following the arguments in Theorem 5.11, the share of pairs of involutions which are mapped to R is

$$\frac{|\varphi^{-1}(R)|}{|i^L \times i^L|} \geqslant \frac{|R||S||C_L(i)|^2}{|L|^2} = \frac{|S|^2|C_L(i)|^2}{|N_L(T)||L|}.$$

Now we shall calculate this quotient in $\mathrm{SL}_4(q)$ and $\mathrm{SU}_4(q)$.

Assume first that $L = \mathrm{SL}_4(q)$. Then a classical involution inverts a torus of order $(q-1)(q+1)$. To see this, let $H = \mathrm{GL}_2(q)$ and

$$j = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in H.$$

Then j inverts tori T_1, $T_2 \leqslant \mathrm{SL}_2(q)$ of order $q-1$ and $q+1$. It is easy to see that $|N_H(T_1)| = 2(q-1)^2$ and $|N_H(T_2)| = 2(q-1)(q+1)$. Now

$$i = \begin{bmatrix} 0 & 1 & & 0 \\ 1 & 0 & & \\ & & 0 & 1 \\ 0 & & 1 & 0 \end{bmatrix} \in \mathrm{SL}_4(q)$$

is a classical involution and i inverts a torus T of order $(q-1)(q+1)$, here T contains a copy of T_1 and T_2. More precisely,

$$\{\begin{bmatrix} t_1 & 0 \\ 0 & t_2 \end{bmatrix} \mid t_k \in T_k,\ k = 1, 2\} \leqslant T.$$

Observe that $|N_L(T)| \geqslant 4(q-1)^2(q+1)$ and one of $(q-1)/2$ or $(q+1)/2$ is an odd number. Therefore the probability of producing an involution from a random element in T is at least $1/2$ and this involution belongs to one of T_1 or T_2 with probability at least $1/2$. Hence with probability at least $1/4$, we can produce an involution belonging to only T_1 or T_2, and it is clear that the involutions in T_1 or T_2 do not centralize the components in $C_L(i)$. Moreover observe that the number of regular elements of even order in T is at least $|S| = |T|/4$. Hence after a simple rearrangement, we have

$$\frac{|\varphi^{-1}(R)|}{|i^L \times i^L|} \geqslant \frac{(q-1)^3(q+1)^3}{64q^2(q^2+1)(q^2+q+1)} \geqslant \frac{1}{64 \cdot 3} = \frac{1}{192}.$$

Now, assume that $L = \mathrm{SU}_4(q)$. Then a classical involution i inverts a torus T of order $(q-1)(q+1)$ and $|N_L(T)| = 4(q-1)(q+1)^2$. Moreover the number of regular elements of even order in T is at least $|S| = |T|/4$ by the same argument. Hence we have

$$\frac{|\varphi^{-1}(R)|}{|i^L \times i^L|} \geqslant \frac{(q-1)^5(q+1)^2}{64q^2(q^2+1)(q^3+1)} \geqslant \frac{1}{64 \cdot 3} = \frac{1}{192}.$$

The computations in the case $L = \mathrm{PSL}_4(q)$ are analogous, namely i inverts a torus T of order $(q-1)(q+1)/(4, q-1)$ and $|N_L(T)| = 4(q-1)^2(q+1)/(4, q-1)$, and we obtain the same lower bound. If $L = \mathrm{PSL}_3(q)$, then the only involution in $C_L(i)$ which centralize the component $\mathrm{SL}_2(q)$ is i. Therefore, for any $g \in L$, if $\zeta_0^i(g) \neq 1$ or equivalently ii^g has even order, then $\zeta_0^i(g)$ does not centralize the component in $C_G(i)$ since ζ_0^i does not produce the involution i itself by Lemma 3.3. The share of elements $g \in L$ such that ii^g has even order is bigger than $1/192$ by the similar computations. The cases $\mathrm{PSU}_n(q)$ for $n = 3, 4$ are analogous. □

Lemma 6.9. *Let $G = \mathrm{PSL}_n^{\varepsilon}(q)$, $n \neq 4$, $K \leqslant G$ be a long root $\mathrm{SL}_2(q)$-subgroup and $i \in K$ be the involution. Let $j \in C_G(i)$ be an involution in the image of the map ζ_0^i which does not centralize K. Then the involution j is a classical involution (that is, of type t_2) and $j \in N_G(K)$.*

Proof. Assume that $G = (\mathrm{P})\mathrm{SL}_n(q)$, the case $G = \mathrm{PSU}_n(q)$ is analogous. Let $n \geqslant 5$ and fix $g \in G$ so that $\zeta_0^i(g) \neq 1$, then the subgroup $\langle K, K^g \rangle$ can be embedded into $\mathrm{SL}_4(q)$. Hence the involution $\zeta_0^i(g)$ belongs to a subgroup isomorphic to $\mathrm{SL}_4(q)$ and there are two types of involutions in $\mathrm{SL}_4(q)$, involutions of type t_2 and t_4 which are classical and central involution in $\mathrm{SL}_4(q)$ respectively. Clearly if $j = \zeta_0^i(g)$ is an involution of type t_4, then j centralizes K. Hence if $\zeta_0^i(g)$ does not centralize K, then it is of type t_2. Since $n \neq 4$, we have $C_G(i) = N_G(K)$ which implies that $j \in N_G(K)$.

If $G = \mathrm{PSL}_3(q)$, then there is only one conjugacy class of involutions which are classical, therefore any involution of type $\zeta_0^i(g)$ is a classical involution. □

Remark 6.10. Let $G = \mathrm{PSL}_4(q)$ and $i \in G$ a classical involution, then the involutions of the form $\zeta_0^i(g)$ are not necessarily classical involutions. However it is clear that the image of $\zeta_0^i(G)$ contains classical involutions. There are three conjugacy classes of involutions which are of type t_1, t_2 (classical) and t_2' in G. Note that involutions of type t_2' exists in G exactly when $q \equiv -1 \bmod 4$ and they are conjugate to

$$j = \begin{bmatrix} & & 1 & \\ & & & 1 \\ -1 & & & \\ & -1 & & \end{bmatrix}.$$

Assume that

$$i = \begin{bmatrix} -1 & & & \\ & -1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}$$

then i is conjugate to

$$t = \begin{bmatrix} & & -1 & \\ & & & -1 \\ -1 & & & \\ & -1 & & \end{bmatrix},$$

say $t = i^g$ for some $g \in G$. Now $j = it = ii^g = \zeta_0^i(g)$ is an involution in $\mathrm{PSL}_4(q)$ which implies that the image of $\zeta_0^i(G)$ contains involutions of type t_2' in $\mathrm{PSL}_4(q)$.

6.2.1 $\mathrm{PSL}_n^{\varepsilon}(q)$, $n \geqslant 3$, $q \geqslant 5$:

In this section we present an algorithm which constructs all long root $\mathrm{SL}_2(q)$-subgroups in a black box group G isomorphic to $\mathrm{PSL}_n(q)$, $n \geqslant 3$, $q \geqslant 5$ which correspond to the nodes in the extended Dynkin diagram of $\mathrm{PSL}_n(q)$. We present the algorithm for $\mathrm{PSL}_n(q)$ and the algorithm for $\mathrm{PSU}_n(q)$ can be read along the same steps by changing the notation SL to SU.

Algorithm 6.11. "Curtis-Tits system for $\mathrm{PSL}_n(q)$"

Input: A black box group G isomorphic to $\mathrm{PSL}_n(q)$, $q \geqslant 5$ odd and $n \geqslant 3$.

Output: Some generators for long root $\mathrm{SL}_2(q)$-subgroups of G which correspond to the nodes in the extended Dynkin diagram of G.

Description of the algorithm:
Step1: Construct a long root $\mathrm{SL}_2(q)$-subgroup K_1.

We use Algorithm 4.1 to construct K_1. Let $i_1 \in Z(K_1)$ be the involution. Assume that $G \neq \mathrm{PSL}_4(q)$, then we have $C_G(i_1) = K_1L_1S_1$ where $[K_1, L_1] = 1$ and S_1 is a torus normalizing K_1 and L_1 whose order is dividing $q-1$, see Lemma 2.18. Moreover $C_G(i_1)' = K_1L_1$ and $L_1 \cong \mathrm{SL}_{n-2}(q)$. If $G = \mathrm{PSL}_4(q)$, then $C = K_1L_1S_1$ is a normal subgroup of index 2 in $C_G(i_1)$ and there is an involution in $C_G(i_1)$ which does not belong to C and interchanges K_1 with L_1, and $C_G(i_1)'' = K_1L_1$.

Step2: Construct the following:

- A classical involution $i_2 \in N_G(K_1) \backslash C_G(K_1)$.
- The long root $\mathrm{SL}_2(q)$-subgroup K_2 where $i_2 \in Z(K_2)$ and $\langle K_1, K_2 \rangle \cong (\mathrm{P})\mathrm{SL}_3(q)$.

We first construct an involution $i_2 \in C_G(i_1)$ which does not centralize K_1 by using the map $\zeta_0^{i_1}$. The existence and frequency of elements producing such involutions follow from Theorem 3.9 and Lemma 6.8. Note that if $G \neq \mathrm{PSL}_4(q)$, then i_2 is a classical involution by Lemma 6.9 and lies in $N_G(K_1)$. If $G = \mathrm{PSL}_4(q)$, then i_2 can be an involution in $C_G(i_1)$ which interchanges K_1 with L_1 which is not a classical involution

in G, indeed, $C_G(i_2)$ contains a normal subgroup C such that $C_G(i_2)/C$ is a dihedral group of order $q+1$ or $2(q+1)$ and $C/Z(C) \cong \mathrm{PSL}_2(q^2)$. We can check whether i_2 is a classical involution by using Algorithm 4.14 and if it is not a classical involution then we search for a classical involution in the same way. The probability of producing a classical involution i_2 is at least $1/192$ by Lemma 6.8. Now $C_G(i_2)'' = K_2L_2$ where K_2 is a long root $\mathrm{SL}_2(q)$-subgroup in G and $L_2 \cong \mathrm{SL}_{n-2}(q)$.

Now we shall prove that $\langle K_1, K_2\rangle \cong (\mathrm{P})\mathrm{SL}_3(q)$. Assume that $G = \mathrm{SL}_n(q)$, $n \geqslant 4$, and V is the natural module for G. Let $V = V_-^1 \oplus V_+^1 = V_-^2 \oplus V_+^2$ where $V_\pm^1$ and $V_\pm^2$ are the eigenspaces of the involutions i_1 and i_2 corresponding to the eigenvalues ± 1. We assume that $dim V_-^1 = dim V_-^2 = 2$ since i_1 and i_2 are classical involutions. Then $\langle i_1, i_2\rangle < \mathrm{SL}(V_-^1 + V_-^2)$. We know that i_2 leaves invariant the subspaces V_-^1, V_+^1 since i_2 normalizes K_1 and $[i_2, V_-^1] \neq 0$ since i_2 does not centralize K_1. If $dim[i_2, V_-^1] = 2$, then $i_1 = i_2$. Therefore we have $dim[i_2, V_-^1] = 1$ which implies that $dim(V_-^1 + V_-^2) = 3$ and $\langle K_1, K_2\rangle \cong \mathrm{SL}_3(q)$.

Hence we have

- $[i_1, i_2] = 1$.
- $i_2 \in N_G(K_1)\backslash C_G(K_1)$.
- $\langle K_1, K_2\rangle \cong \mathrm{SL}_3(q)$. If $n = 3$, then $\langle K_1, K_2\rangle \cong \mathrm{PSL}_3(q)$.

We use the same method in Step3 of Algorithm 5.13 to construct K_2 in the commuting product $C_2 = K_2L_2$.

If $G = \mathrm{PSL}_3(q)$, then the involution $i_3 = i_1 \cdot i_2$ is a classical involution and it is clear that $i_3 \in N_G(K_s)\backslash C_G(K_s)$ for $s = 1, 2$. Let $K_3 = C_G(i_3)'$ be the corresponding long root $\mathrm{SL}_2(q)$-subgroup. Then $\langle K_1, K_2\rangle = \langle K_2, K_3\rangle = \langle K_3, K_1\rangle = \mathrm{PSL}_3(q)$. Here the subgroups K_1 and K_2 correspond to the nodes in the Dynkin diagram while the subgroup K_3 corresponds the extra node in the extended Dynkin diagram.

If $G = \mathrm{PSL}_4(q)$, then we have $\langle K_1, K_2\rangle = \langle K_2, L_1\rangle = \langle L_1, L_2\rangle = \mathrm{SL}_3(q)$ and $[K_1, L_1] = [K_2, L_2] = 1$. Therefore the subgroups K_1, K_2, L_1 correspond to the nodes in the Dynkin diagram while the subgroup L_2 corresponds the extra node.

Step3: Construct long root $\mathrm{SL}_2(q)$-subgroups K_l such that $\langle K_l, K_{l+1}\rangle \cong \mathrm{SL}_3(q)$ for $l = 1, \ldots, n-1$ and $\langle K_s, K_t\rangle = 1$ where $|s-t| \geqslant 2$.

We can assume now that $n \geqslant 5$. We work in the subgroup $L_1 \cong \mathrm{SL}_{n-2}(q)$. By the above construction we have $i_2 \in N_G(L_1)$ and $i_2 \notin C_G(L_1)$. Moreover i_2 acts as an involution of type t_1 on L_1 since it is a classical involution in G and $i_2 \notin C_G(L_1)$. Now we construct an involution $i_3 = \zeta_0^{i_2}(g)$ with the property that $i_3 \notin C_G(K_2)$ for some $g \in L_1$. It is clear that $i_3 \in L_1$ since $i_2 \in N_G(L_1)$ and $g \in L_1$. The involution i_3 is classical involution in L_1 by Lemma 6.9. Therefore $C_{L_1}(i_3)' = K_3L_3$. We have

- $[i_s, i_t] = 1$ for $s, t = 1, 2, 3$.
- $i_{s+1} \in N_G(K_s)\backslash C_G(K_s)$ for $s = 1, 2$.
- $\langle K_s, K_{s+1}\rangle \cong \mathrm{SL}_3(q)$ for $s = 1, 2$ and $\langle K_1, K_3\rangle = 1$.

We construct $\tilde{L}_2 = C_{L_1}(i_2)''$ and work in this subgroup. Clearly $\tilde{L}_2 < L_2$ and $\tilde{L}_2 \cong \mathrm{SL}_{n-3}(q)$ since i_2 acts an involution of type t_1 on L_1, see Table 2.5. Therefore $[\tilde{L}_2, K_1] = [\tilde{L}_2, K_2] = 1$. Now we construct an involution i_4 by using $\zeta_0^{i_3}$ in $\tilde{L}_2$ with the property that $i_4 \notin C_G(K_3)$ for some $g \in \tilde{L}_2$. By the same argument i_4 is a classical involution in $\tilde{L}_2$ and hence $C_{\tilde{L}_2}(i_4)' = K_4L_4$. We have

- $[i_s, i_t] = 1$ for $s, t = 1, 2, 3, 4$.
- $i_{s+1} \in N_G(K_s)\backslash C_G(K_s)$ for $s = 1, 2, 3$.
- $\langle K_s, K_{s+1}\rangle \cong \mathrm{SL}_3(q)$, $s = 1, 2, 3$ and $\langle K_s, K_t\rangle = 1$ where $|s-t| \geqslant 2$.

Now we construct $\tilde{L}_3 = C_{\tilde{L}_2}(i_3)'$ and work in this subgroup in the same way as above. Observe that $\tilde{L}_{n-3} \cong \mathrm{SL}_2(q)$ which corresponds to the end node in the Dynkin diagram, say $\tilde{L}_{n-3} = K_{n-1}$.

Step4: Construct a long root $\mathrm{SL}_2(q)$-subgroup corresponding to extra node in the extended Dynkin diagram.

Let $i_n = i_1 \cdot i_2 \cdots i_{n-1}$. Then it is easy to see that i_n is a classical involution and $i_n \in N_G(K_{n-1})\backslash C_G(K_{n-1})$. Let K_n be the corresponding long root $\mathrm{SL}_2(q)$-subgroup containing i_n, then $\langle K_{n-1}, K_n\rangle \cong \mathrm{SL}_3(q)$ and $[K_s, K_n] = 1$ for $s = 2, 3, \ldots, n-2$. Notice that $i_n \in N_G(K_1)\backslash C_G(K_1)$. Hence K_n corresponds to the extra node in the extended Dynkin diagram.

Hence we have constructed the following.

- $\langle K_s, K_{s+1}\rangle = (\mathrm{P})\mathrm{SL}_3(q)$ for $s = 1, \ldots, n-1$.
- $[K_s, K_t] = 1$ if $|s-t| \geqslant 2$ and $s, t = 1, \ldots, n-1$.
- $\langle K_n, K_1\rangle \cong \langle K_n, K_{n-1}\rangle(\mathrm{P})\mathrm{SL}_3(q)$.
- $[K_n, K_s] = 1$ for $s = 2, 3, \ldots, n-2$.

Therefore the subgroups K_s, $s = 1, \ldots, n$, correspond to the nodes in the extended Dynkin diagram of $(\mathrm{P})\mathrm{SL}_n(q)$, see Table 2.1. Let T_1 be a maximal torus of order $q-1$ in K_1 and T_s be the maximal torus of K_s normalizing K_{s-1} and centralizing T_{s-1} for each $s = 2, 3, \ldots, n-1$. Then $T = \langle T_s \mid s = 1, \ldots, n-1\rangle$ is a maximal torus of order $(q-1)^{n-1}$ in G, hence it is a maximal standard torus of G, that is, $T \leqslant N_G(K_s)$ for each $s = 1, \ldots, n-1$.

In the case of $G = (\mathrm{P})\mathrm{SU}_n(q)$, we consider the tori T_s of orders $q+1$ in K_s for $s = 1, \ldots, n-1$. Following the same construction as above, $T = \langle T_s \mid s = 1, \ldots, n-1\rangle$ is a maximal torus of order $(q+1)^{n-1}$ in G, and $T \leqslant N_G(K_s)$ for each $s = 1, \ldots, n-1$, that is, T is a maximal standard torus of G. Hence we have constructed the Curtis-Phan-Tits system for the groups $(\mathrm{P})\mathrm{SL}_n^{\varepsilon}(q)$.

References

[1] Christine Altseimer and Alexandre V. Borovik. Probabilistic recognition of orthogonal and symplectic groups. In *Groups and computation, III (Columbus, OH, 1999)*, volume 8 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 1–20. de Gruyter, Berlin, 2001.

[2] E. Artin. *Geometric algebra*. Interscience Publishers, Inc., New York-London, 1957.

[3] M. Aschbacher. A characterization of Chevalley groups over fields of odd order. I, II. *Ann. of Math. (2)*, 106(3):353–468, 1977.

[4] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math.*, 76(3):469–514, 1984.

[5] Michael Aschbacher. *Finite group theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, second edition, Cambridge, 2000.

[6] L. Babai. Local expansion of vertex-transitive graphs and random generation in finite groups. *Proc. ACM Symp. on Theory of Computing*, pages 164–174, 1991.

[7] L. Babai and R. Beals. A polynomial-time theory of black box groups. I. In *Groups St. Andrews 1997 in Bath, I*, volume 260 of *London Math. Soc. Lecture Note Ser.*, pages 30–64. Cambridge Univ. Press, Cambridge, 1999.

[8] L. Babai, G. Cooperman, L. Finkelstein, E. Luks, and Á. Seress. Fast Monte Carlo algorithms for permutation groups. *J. Comput. System Sci.*, 50(2):296–308, 1995. 23rd Symposium on the Theory of Computing (New Orleans, LA, 1991).

[9] L. Babai, W. M. Kantor, P. P. Pálfy, and Á. Seress. Black-box recognition of finite simple groups of Lie type by statistics of element orders. *J. Group Theory*, 5(4):383–401, 2002.

[10] L. Babai and A. Shalev. Recognizing simplicity of black-box groups and the frequency of p-singular elements in affine groups. In *Groups and computation, III (Columbus, OH, 1999)*, volume 8 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 39–62. de Gruyter, Berlin, 2001.

[11] L. Babai and E. Szemerédi. On the complexity of matrix group problems. *Proc. 25th IEEE Sympos. Foundations Comp. Sci.*, pages 229–240, 1984.

[12] C. D. Bennett and S. Shpectorov. A new proof of a theorem of Phan. *J. Group Theory*, 7(3):287–310, 2004.

[13] A. V. Borovik. Centralisers of involutions in black box groups. In *Computational and statistical group theory (Las Vegas, NV/Hoboken, NJ, 2001)*, volume 298 of *Contemp. Math.*, pages 7–20. Amer. Math. Soc., Providence, RI, 2002.

[14] J. N. Bray. An improved method for generating the centralizer of an involution. *Arch. Math. (Basel)*, 74(4):241–245, 2000.

[15] P. A. Brooksbank. Fast constructive recognition of black-box unitary groups. *LMS J. Comput. Math.*, 6:162–197 (electronic), 2003.

[16] P. A. Brooksbank and W. M. Kantor. On constructive recognition of a black box $\mathrm{PSL}(d, q)$. In *Groups and computation, III (Columbus, OH, 1999)*, volume 8 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 95–111. de Gruyter, Berlin, 2001.

[17] P. A. Brooksbank and W. M. Kantor. Fast constructive recognition of black box orthogonal groups. *J. Algebra*, 300(1):256–288, 2006.

[18] R. Carter. Conjugacy classes in the Weyl group. In *Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69)*, pages 297–318. Springer, Berlin, 1970.

[19] R. W. Carter. *Simple groups of Lie type*. John Wiley & Sons, London-New York-Sydney, 1972. Pure and Applied Mathematics, Vol. 28.

[20] R. W. Carter. *Finite groups of Lie type: Conjugacy classes and complex characters*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, 1985.

[21] F. Celler and C. R. Leedham-Green. A constructive recognition algorithm for the special linear group. In *The atlas of finite groups: ten years on (Birmingham, 1995)*, volume 249 of *London Math. Soc. Lecture Note Ser.*, pages 11–26. Cambridge Univ. Press, Cambridge, 1998.

[22] F. Celler, C. R. Leedham-Green, S. H. Murray, A. C. Niemeyer, and E. A. O'Brien. Generating random elements of a finite group. *Comm. Algebra*, 23(13):4931–4948, 1995.

[23] M. D. E. Conder, C. R. Leedham-Green, and E. A. O'Brien. Constructive recognition of $\mathrm{PSL}(2, q)$. *Trans. Amer. Math. Soc.*, 358(3):1203–1221 (electronic), 2006.

[24] G. Cooperman, L. Finkelstein, and S. Linton. Constructive recognition of a black box group isomorphic to $\mathrm{GL}(n, 2)$. In *Groups and computation, II (New Brunswick, NJ, 1995)*, volume 28 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 85–100. Amer. Math. Soc., Providence, RI, 1997.

[25] D. Gorenstein, R. Lyons, and R. Solomon. *The classification of the finite simple groups. Number 3. Part I. Chapter A*, volume 40 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1998.

[26] R. L. Griess, Jr. Finite groups whose involutions lie in the center. *Quart. J. Math. Oxford Ser. (2)*, 29(115):241–247, 1978.

[27] The GAP Group. Gap - groups, algorithms, and programming, version 4.2. *Aachen, St Andrews*, (`http://www-gap.dcs.st-and.ac.uk/ gap`), 2000.

[28] R. M. Guralnick and F. Lübeck. On p-singular elements in Chevalley groups in characteristic p. In *Groups and computation, III (Columbus, OH, 1999)*, volume 8 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 169–182. de Gruyter, Berlin, 2001.

[29] R. M. Guralnick and P. H. Tiep. Finite simple unisingular groups of Lie type. *J. Group Theory*, 6(3):271–310, 2003.

[30] J. E. Humphreys. *Linear algebraic groups*. Springer-Verlag, New York, 1975. Graduate Texts in Mathematics, No. 21.

[31] I. M. Isaacs, W. M. Kantor, and N. Spaltenstein. On the probability that a group element is p-singular. *J. Algebra*, 176(1):139–181, 1995.

[32] N. Iwahori. Centralizers of involutions in finite Chevalley groups. In *Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69)*, Lecture Notes in Mathematics, Vol. 131, pages 267–295. Springer, Berlin, 1970.

[33] W. M. Kantor and A. Lubotzky. The probability of generating a finite classical group. *Geom. Dedicata*, 36(1):67–87, 1990.

[34] W. M. Kantor and Á. Seress. Black box classical groups. *Mem. Amer. Math. Soc.*, 149(708):viii+168, 2001.

[35] W. M. Kantor and Á. Seress. Prime power graphs for groups of Lie type. *J. Algebra*, 247(2):370–434, 2002.

[36] C. R. Leedham-Green. The computational matrix group project. In *Groups and computation, III (Columbus, OH, 1999)*, volume 8 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 229–247. de Gruyter, Berlin, 2001.

[37] M. W. Liebeck and G. M. Seitz. Subgroups generated by root elements in groups of Lie type. *Ann. of Math. (2)*, 139(2):293–361, 1994.

[38] M. W. Liebeck and A. Shalev. The probability of generating a finite simple group. *Geom. Dedicata*, 56(1):103–113, 1995.

[39] M. W. Liebeck and A. Shalev. Diameters of finite simple groups: sharp bounds and applications. *Ann. of Math. (2)*, 154(2):383–406, 2001.

[40] A. Lubotzky and I. Pak. The product replacement algorithm and Kazhdan's property (T). *J. Amer. Math. Soc.*, 14(2):347–363 (electronic), 2001.

[41] D. S. Mitrinović, J. Sándor, and B. Crstici. *Handbook of number theory*, volume 351 of *Mathematics and its Applications*. Kluwer Academic Publishers Group, Dordrecht, 1996.

[42] Peter M. Neumann and Cheryl E. Praeger. A recognition algorithm for special linear groups. *Proc. London Math. Soc. (3)*, 65(3):555–603, 1992.

[43] I. Pak. The product replacement algorithm is polynomial. *Proc. FOCS'2000, The 41st Ann. Symp. on Foundations of Comp. Sci.*, pages 476–485, 2001.

[44] Igor Pak. What do we know about the product replacement algorithm? In *Groups and computation, III (Columbus, OH, 1999)*, volume 8 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 301–347. de Gruyter, Berlin, 2001.

[45] K. W. Phan. On groups generated by three-dimensional special unitary groups. I, II. *J. Austral. Math. Soc. Ser. A*, 23(1):67–77, 129–146, 1977.

[46] Á. Seress. *Permutation group algorithms*, volume 152 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2003.

[47] R. Steinberg. *Lectures on Chevalley groups*. Yale University, New Haven, Conn., 1968. Notes prepared by John Faulkner and Robert Wilson.

[48] F. G. Timmesfeld. The Curtis-Tits-presentation. *Adv. Math.*, 189(1):38–67, 2004.

VITA

PERSONAL INFORMATION

Surname, Name: Yalçınkaya, Şükrü
Nationality: Turkish (T. C.)
Date and Place of Birth: 27 June 1977, Çanakkale
Marital Status: Single
email: sukru.yalcinkaya@gmail.com

EDUCATION

Degree	Institution	Year of Graduation
MS	METU, Mathematics	2001
BS	METU, Mathematics	1999
High School	Suphi Koyuncuğlu Lisesi	1994

WORK EXPERIENCE

Year	Place	Enrollment
2006-2007 Fall	METU Northern Cyprus Campus,	Teaching Assistant
1999-2006	METU, Mathematics	Teaching Assistant

FOREIGN LANGUAGE

English

ACADEMIC VISITS AND GRANTS

1. August 2003 - August 2004, University of Manchester, United Kingdom, grant obtained from The Scientific and Technological Research Council of Turkey(TÜBİTAK)
2. September 2005 - November 2005, Université Claude Bernard - Lyon 1, France, grant obtained from Mathlogaps

CONFERENCE TALKS

1. Some important classification theorems in 20th century algebra, National Mathematics Symposium XIII, Istanbul, Turkey, September 2000
2. Recognition of the p-core in finite groups, Antalya Algebra Days VII, Antalya, Turkey, May 2005
3. Black box recognition of finite groups and related group theoretic constructions, Asymptotic Group Theory, The Hebrew University of Jerusalem, May 2006
4. Black box recognition of finite groups and related group theoretic constructions, Computational Group Theory, Oberwolfach, Germany, July 2006
5. Black box recognition of finite groups and related group theoretic constructions, MODNET, Antalya, Turkey, November 2006
6. From proofs about finite groups to probabilistic algorithms for black box groups, Antalya Algebra Days IX, Antalya, Turkey, May 2007